

Guia do Usuário do Nessus 5.0 HTML5

4 de dezembro de 2012

(Revisão 4)

Índice

Introdução	3
Padrões e convenções	3
Descrição da interface do usuário Nessus	3
Descrição	3
Plataformas compatíveis.....	4
Instalação	4
Operação	4
Visão geral	4
Conexão com a interface do usuário Nessus	4
Visão geral das políticas	10
Políticas padrão	10
Como criar uma nova política.....	11
General Settings (Configurações gerais)	12
Credentials (Credenciais)	15
Plugins.....	21
Preferences (Preferências)	25
Importar, exportar e copiar políticas	28
Criar, iniciar e programar uma varredura.....	29
Results (Resultados)	33
Procurar resultados de varreduras.....	34
Filtros de relatórios	37
Comparar (diferenciar resultados).....	42
Upload e download (exportar)	44
Formato de arquivo .nessus.....	45
Delete (Excluir)	45
Móvel	46
SecurityCenter	46
Configuração do SecurityCenter 4.0-4.2 para funcionar com o Nessus	46
Configuração do SecurityCenter 4.4 para funcionar com o Nessus	47
Firewalls instalados no host.....	48
Verificação de preferências detalhadas.....	49
Para obter mais informações.....	75
Sobre a Tenable Network Security	77

Introdução

Este documento descreve como usar a **interface do usuário Nessus (UI)** da Tenable Security Network. Envie seus comentários e sugestões para o e-mail support@tenable.com.

A interface do usuário Nessus é uma interface baseada na Web que complementa o scanner de vulnerabilidades Nessus. Para usar o cliente, é preciso um scanner Nessus em operação instalado e estar familiarizado com o seu uso.

Padrões e convenções

Este documento é a tradução de uma versão original em inglês. Algumas partes do texto permanecem em inglês para indicar a representação do próprio produto.

Em toda a documentação, os nomes de arquivos, daemons e executáveis são indicados com a fonte **courier bold**, por exemplo, **gunzip**, **httpd** e **/etc/passwd**.

As opções de linha de comando e palavras-chaves também são impressas indicadas com a fonte **courier bold**. Os exemplos de linhas de comando podem ou não conter o prompt da linha de comando e o texto gerado pelos resultados do comando. Os exemplos de linhas de comando exibirão o comando executado em **courier bold** para indicar o que o usuário digitou, enquanto que o exemplo de saída gerado pelo sistema será indicado em **courier** (sem negrito). Um exemplo da execução do comando **pwd** do Unix é apresentado a seguir:

```
# pwd
/opt/nessus/
#
```



As observações e considerações importantes são destacadas com este símbolo nas caixas de texto escurecidas.



As dicas, exemplos e práticas recomendados são destacados com este símbolo em branco sobre fundo azul.

Descrição da interface do usuário Nessus

Descrição

A interface do usuário Nessus (UI) é uma interface baseada na Web desenvolvida para o scanner Nessus, que consiste em um servidor HTTP simples e um cliente da Web e dispensa a instalação de qualquer software além do servidor Nessus. A partir do Nessus 4, todas as plataformas aproveitam o mesmo código básico, eliminando a maioria dos erros específicos de plataforma e acelerando a implementação de novos recursos. Os recursos principais são:

- Gera arquivos **.nessus** usados pelos produtos da Tenable como padrão de dados de vulnerabilidades e políticas de varredura.
- Uma sessão de política, lista de alvos e os resultados de várias varreduras podem ser armazenados em um único arquivo **.nessus**. Consulte o guia de formatos de arquivos do Nessus para obter mais detalhes.
- A interface do usuário exibe, em tempo real, os resultados das varreduras, de modo que não seja preciso esperar a conclusão de uma varredura para ver os resultados.
- Unifica a interface do scanner Nessus, independentemente da plataforma de base. As mesmas funções existem no Mac OS X, Windows e Linux.
- As varreduras continuarão sendo executadas no servidor, mesmo se o usuário for desconectado por qualquer motivo.

- Os relatórios de varredura do Nessus podem ser carregados por meio da interface do usuário Nessus e comparados a outros relatórios.

Plataformas compatíveis

- Como a interface do usuário Nessus é um cliente da Web, ela funciona em qualquer plataforma com um navegador moderno.



Para melhor desempenho, a interface do usuário baseada na Web do Nessus deve ser visualizada com o Microsoft Internet Explorer 9 e 10, Mozilla Firefox 15.x, Google Chrome 16.x, Opera 12.x ou Apple Safari 5.x.

Instalação

O gerenciamento do servidor Nessus 5 pelo usuário é realizado por uma interface baseada na Web ou SecurityCenter e dispensa o uso de um NessusClient autônomo. O NessusClient autônomo continua a conectar e operar o scanner, mas deixará de ser atualizado ou oferecer suporte.

Consulte o Guia de Instalação e Configuração do Nessus 5.0 para obter instruções sobre como instalar o Nessus. A partir do Nessus 5.0, o [Oracle Java](#) (conhecido como Java da Sun Microsystems) é necessário para a funcionalidade de relatórios no formato PDF.

Operação

Visão geral

O Nessus oferece uma interface simples, mas poderosa, para gerenciar as atividades de varredura de vulnerabilidades.

Conexão com a interface do usuário Nessus

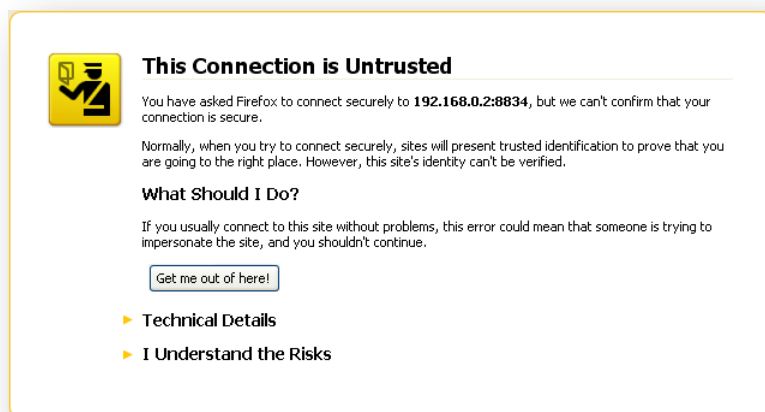
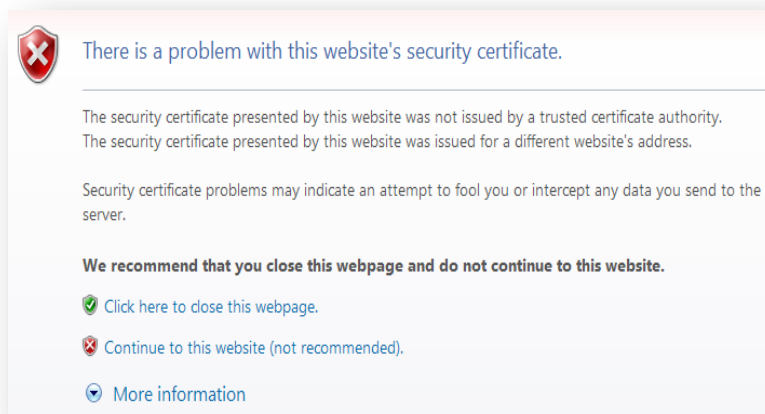
Para iniciar a interface do usuário Nessus HTML5, proceda da seguinte maneira:

- Abra o navegador de sua preferência.
- Digite `https://[server IP]:8834/html5.html#/` na barra de navegação.

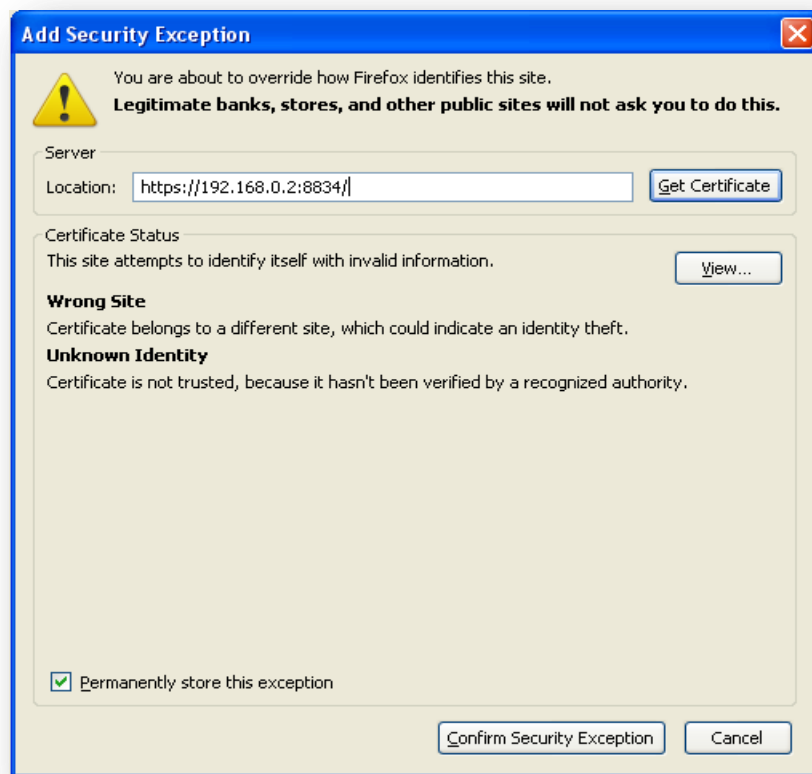


Certifique-se de se conectar à interface do usuário por meio de HTTPS, pois não são permitidas conexões HTTP sem criptografia.

Ao tentar se conectar à interface do usuário Nessus pela primeira vez, a maioria dos navegadores exibirá um erro indicando que o site não é confiável, devido ao certificado SSL autoassinado:

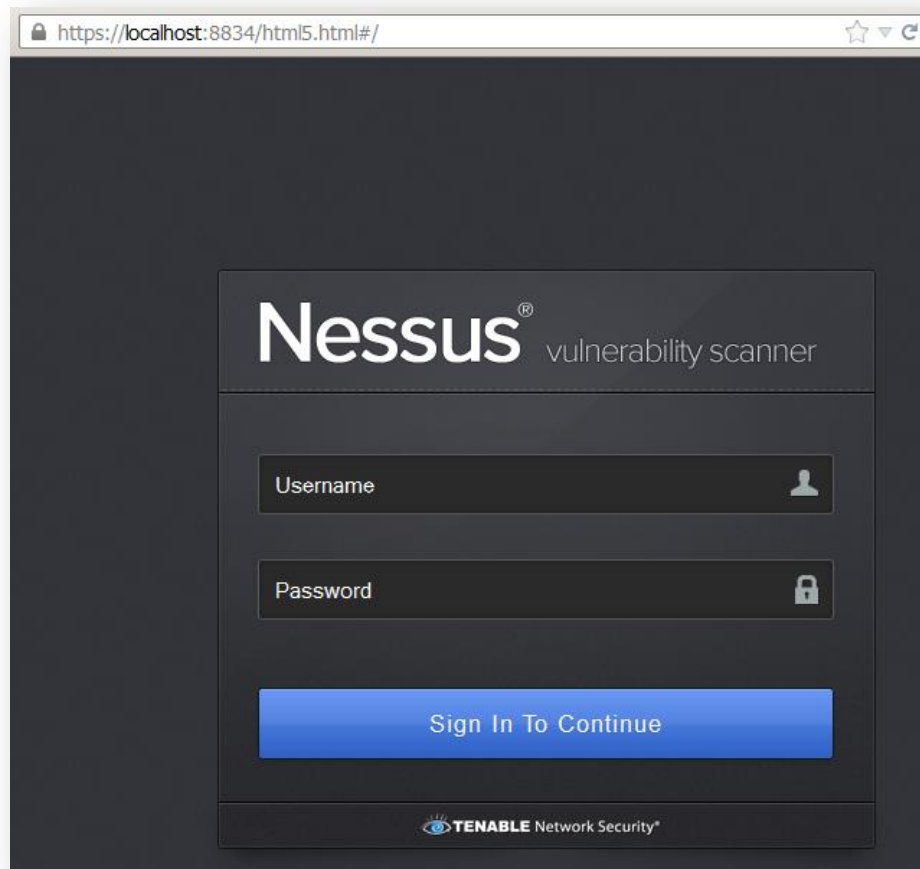


Os usuários do Microsoft Internet Explorer podem clicar em “Continue to this website (not recommended)” (Prosseguir para o website (não recomendado)) para carregar a interface do usuário Nessus. Os usuários do Firefox 3.x – 16.x podem clicar em “I Understand the Risks” (Eu compreendo os riscos) e, em seguida, em “Add Exception...” (Adicionar exceção...) para abrir a caixa de diálogo de exceções de sites:

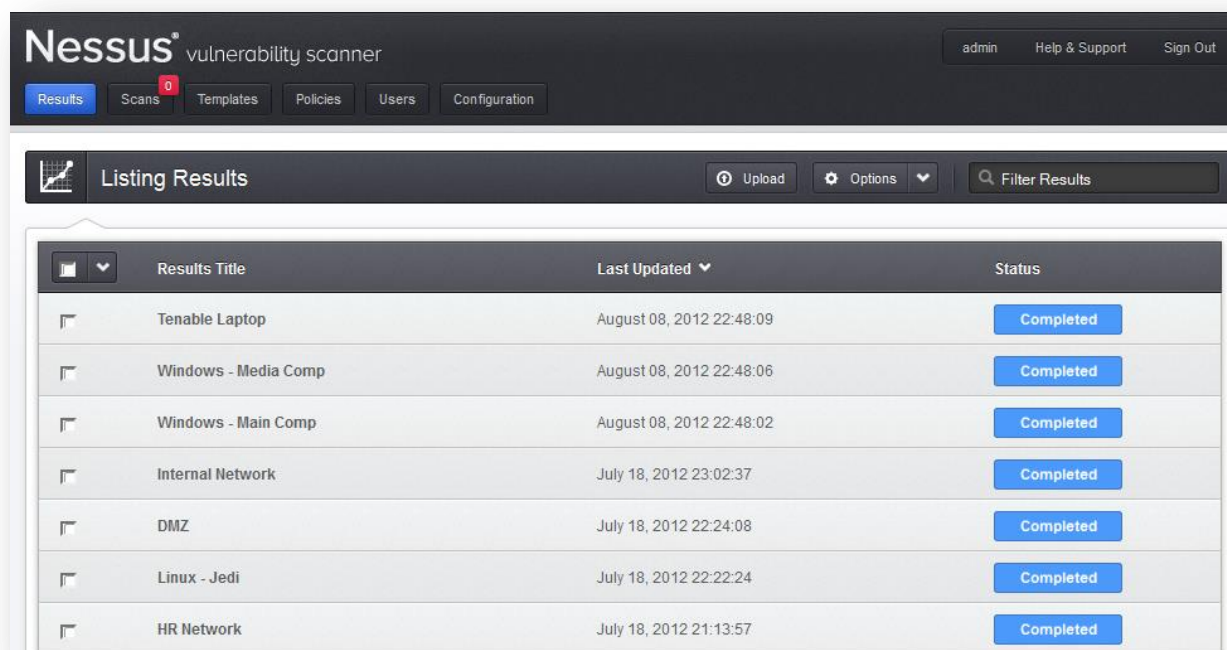


Verifique se a barra “Local:” indica a URL do servidor Nessus e clique em “**Confirm Security Exception**” (Confirmar exceção de segurança). Para obter mais informações sobre como instalar um certificado SSL personalizado, consulte o Guia de Instalação e Configuração do Nessus.

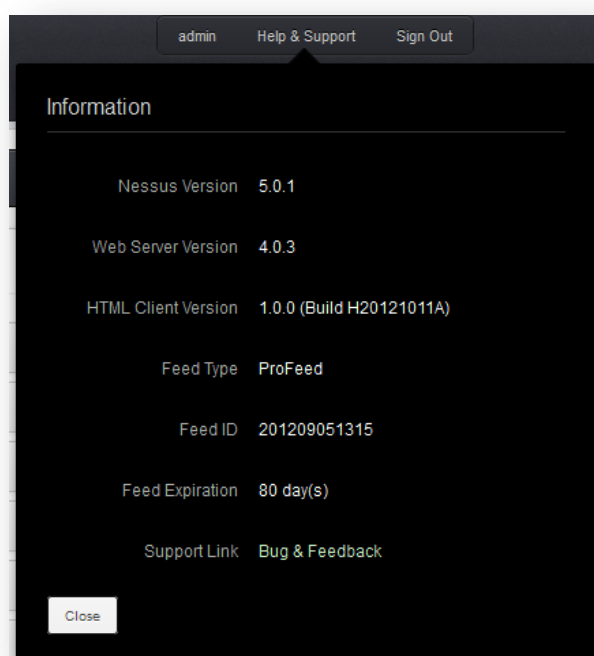
Depois que o navegador confirmar a exceção, a seguinte tela de abertura será exibida:



Autentique-se usando a conta e senha de administrador criadas com o gerenciador do servidor durante o processo de instalação. Após a autenticação, a interface do usuário exibirá os menus para navegação em relatórios, realização de varreduras e gerenciamento de políticas. Os usuários administrativos também terão opções para gerenciamento de usuários e configuração do scanner Nessus:



Em qualquer ponto durante o uso do Nessus, as opções no canto superior esquerdo estarão presentes. A notação “admin” localizada no canto superior direito da imagem acima corresponde à conta conectada no momento. Clique nessa conta para alterar a senha atual. O botão “**Help & Support**” (Ajuda e suporte) exibe informações sobre a instalação do Nessus, incluindo versão, versão do servidor web, versão do cliente HTML, tipo de feed, ID de feed, vencimento do feed e um link para enviar relatórios de bugs ou feedback geral. “**Sign Out**” (Sair) encerrará a sessão atual.



A interface HTML5 tem diversas teclas de atalho que permitirão a navegação rápida com teclado para as seções principais da interface, e também executar rotinas comuns. Podem ser usadas em qualquer ocasião, a partir de qualquer lugar na interface:

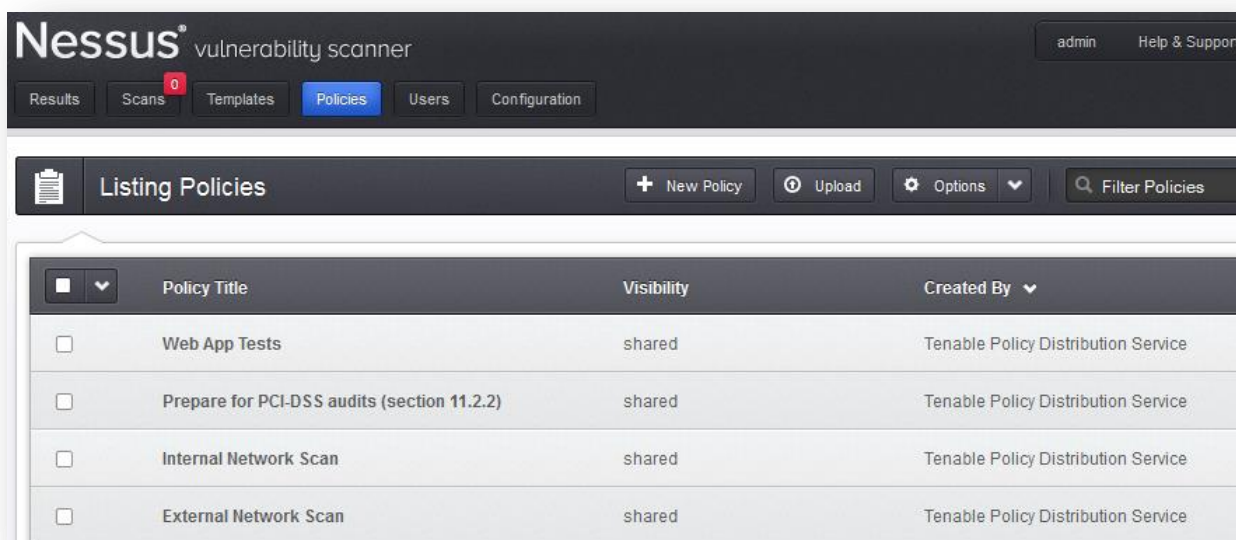
Interface principal	
R	Resultados
S	Varreduras
T	Modelos
P	Políticas
U	Usuários
C	Configuração
Shift + Seta para esquerda/direita	Alterna tabulações para esquerda ou direita
Shift + S	Nova varredura
Exibições de lista	
Shift + Seta para cima/baixo	Move a seleção para cima ou para baixo
Shift + Enter	Abre a entrada selecionada
Exibição de resultados	
Shift + U	Upload de relatório
Esc	Voltar à exibição de resultados
Seta para esquerda/direita	Vulnerabilidade próxima/anterior em modo de detalhes
D	Excluir resultado selecionado
Exibição de varredura	
N	Nova varredura
Exibição de políticas	
Shift + U	Upload de nova política
Exibição de usuário	
N	Novo usuário

Visão geral das políticas

Uma “política” do Nessus consiste em opções de configuração relacionadas à realização de uma varredura de vulnerabilidades. Algumas das opções são, entre outras, as seguintes:

- Parâmetros que controlam aspectos técnicos da varredura, como intervalos de tempo, número de hosts, tipo de scanner de porta etc.
- Credenciais para varreduras locais (por exemplo, Windows, SSH), varreduras autenticadas de bancos de dados Oracle, HTTP, FTP, POP, IMAP ou autenticação pelo Kerberos.
- Especificações individualizadas de varreduras por família ou plugin.
- Verificações de políticas de conformidade de bancos de dados, detalhamento do relatório, definições de varredura de detecção de serviços, verificações de conformidade de Unix, entre outras opções.

Políticas padrão



O Nessus é distribuído com várias políticas padrão criadas pela Tenable Network Security, Inc. As políticas são fornecidas como modelos para ajudá-lo a criar políticas adequadas à sua organização ou para serem usadas sem modificações para varreduras básicas dos seus recursos. Leia e entenda as políticas padrão antes de utilizá-las em varreduras com os seus recursos.

Nome da política	Descrição
Varredura de rede externa	Esta política foi projetada para a verificação de hosts externos e que normalmente apresentam menos serviços à rede. Os plugins relacionados a vulnerabilidades conhecidas de aplicativos da Web (as famílias de plugins CGI Abuses e CGI Abuses: XSS) são ativados com a aplicação desta política. Além disso, todas as 65.536 portas (inclusive a porta 0 por meio de plugin separado) são examinadas em cada destino.
Varredura de rede interna	Esta política foi projetada levando-se em conta a melhoria do desempenho, pois pode ser usada para verificar redes internas de grande porte com muitos hosts, vários serviços expostos e sistemas incorporados, como impressoras. As varreduras de CGI estão desabilitadas e um conjunto de portas padrão é examinado, mas não todas as 65.535.

Testes de aplicativos da Web	Esta política de varredura é usada para verificar os sistemas e fazer com que o Nessus detecte vulnerabilidades conhecidas e desconhecidas nos aplicativos da Web. Os recursos de “difusão” do Nessus são ativados com esta política, o que fará com que o Nessus detecte todos os websites descobertos e verifique as vulnerabilidades presentes em cada um dos parâmetros, incluindo XSS, SQL, injeção de comandos e vários outros. Esta política identificará os problemas via HTTP e HTTPS.
Preparar para auditorias de PCI DSS	Esta política ativa as verificações de conformidade com a norma PCI DSS integradas, compara os resultados das varreduras com os padrões PCI e gera um relatório sobre o comportamento da conformidade. É importante observar que uma varredura de compatibilidade bem-sucedida não garante a conformidade nem uma infraestrutura segura. As organizações que estejam se preparando para uma avaliação da PCI DSS podem usar essa política para preparar suas redes e seus sistemas para a conformidade com a PCI DSS.



Se você pretende usar uma política padrão fornecida pelo Tenable como base para a sua própria política personalizada, use o recurso Copy (Copiar). A edição de uma política padrão fará com que se torne propriedade do usuário e não seja mais exibida na interface.

Como criar uma nova política

Depois de se conectar à interface de usuário do servidor Nessus, é possível criar uma política personalizada ao clicar na opção “**Políticas**” (Políticas) na barra superior e no botão “**+ Add**” (Adicionar) à direita. A tela de adição de política é exibida como no exemplo a seguir:

Nessus vulnerability scanner

admin Help & Support Sign Out

Results Scans Templates **Policies** Users Configuration

Filter Options

General Settings

Policy General Settings

Setting Type: Basic

Name:

Visibility: private

Description:

Allow Post-Scan Report Editing: ☒

Update Cancel

© 1998 - 2012 Tenable Network Security®. All Rights Reserved. Nessus Version: 5.0.1 - ProFeed

Observe que existem quatro guias de configuração: **General** (Geral), **Credentials** (Credenciais), **Plugins** e **Preferences** (Preferências). Na maioria dos ambientes, não é necessário modificar as configurações padrão, mas elas permitem um controle mais individualizado sobre o funcionamento do scanner Nessus. Essas guias são descritas a seguir.

General Settings (Configurações gerais)

A guia “**General Settings**” (Configurações gerais) permite nomear a política e configurar as operações de varredura. Há quatro itens de menu suspenso que controlam o comportamento do scanner:

A tela “**Basic**” (Básico) é usada para definir os aspectos da política em si:

Opção	Descrição
Name (nome)	Define o nome a ser exibido na interface do usuário Nessus para identificar a política.
Visibility (Visibilidade)	Controla se a política é compartilhada com outros usuários (<i>shared</i>) ou mantida somente para uso <i>privado</i> (<i>private</i>). Somente usuários administrativos podem compartilhar políticas.
Description (Descrição)	Oferece uma breve descrição da política de varredura para resumir a finalidade geral (por exemplo, “varreduras em servidores da Web sem verificações locais ou serviços não HTTP”).
Allow Post-Scan Report Editing (Permitir edição do relatório depois da varredura)	Este recurso permite aos usuários excluir itens do relatório quando marcados. Ao fazer uma varredura para conformidade regulatória ou outros tipos de auditoria, esta opção deve ser desmarcada para confirmar que a varredura não foi adulterada.

O menu “**Port Scanners**” (Varredura de portas) controla as opções relacionadas a varreduras de portas, incluindo os intervalos de portas e métodos:

A opção “**Port Scan Range**” (Intervalo de varredura de portas) instrui o scanner a localizar um intervalo de portas específico. Os seguintes valores são permitidos:

Valor	Descrição
“default”	Se a palavra-chave “default” for usada, o Nessus examinará cerca de 4.790 portas comuns. A lista de portas pode ser encontrada no arquivo <code>nessus-services</code> .
“all”	Se a palavra-chave “all” for usada, o Nessus examinará todas as 65.535 portas.
Custom List	Um intervalo personalizado de portas pode ser selecionado com o uso de uma lista delimitada por vírgulas de portas ou intervalos de portas. Por exemplo, é possível usar “21,23,25,80,110” ou “1-1024,8080,9000-9200”. A opção “1-65535” verificará todas as portas. Pode-se especificar também um intervalo de divisão específico para cada protocolo. Por exemplo, para verificar um intervalo de portas diferente para TCP e UDP na mesma política, é preciso especificar “T:1-1024,U:300-500”. Pode-se especificar também um conjunto de portas para varredura em ambos os protocolos, bem como intervalos individuais para cada protocolo separado (“1-1024,T:1024-65535,U:1025”). Se um único protocolo for verificado, selecione somente o scanner para aquela porta e especifique as portas normalmente.

As outras opções disponíveis são:

Opção	Descrição
Consider Unscanned Ports as Closed	Se uma porta não for examinada com um scanner de porta selecionado (por exemplo, fora do intervalo especificado), será considerada fechada pelo Nessus.
Nessus SNMP Scanner	Instrui o Nessus a examinar alvos para um serviço de SNMP. O Nessus detectará as configurações de SNMP correspondentes durante a varredura. Se as configurações forem feitas pelo usuário em “Preferences” (Preferências), o Nessus examinará totalmente o host remoto e produzirá resultados de auditoria mais detalhados. Por exemplo, muitas verificações do roteador Cisco determinam as vulnerabilidades presentes ao examinar a versão do string SNMP devolvido. Essas informações são necessárias para as auditorias.
Nessus UDP Scanner	Esta opção usa o scanner de UDP integrado do Nessus para identificar as portas UDP abertas nos alvos.  O UDP é um protocolo “sem estado”, ou seja, a comunicação não é feita com diálogos de reconhecimento. A comunicação por UDP nem sempre é confiável e, devido à natureza dos serviços UDP e dos dispositivos de rastreamento, nem sempre são detectáveis de maneira remota.
netstat portscanner (SSH)	Esta opção usa o netstat para verificar se há portas abertas no computador local. Depende da disponibilidade do comando netstat por meio de uma conexão SSH com o alvo. Esta varredura se destina a sistemas do tipo Unix e requer credenciais de autenticação.
Ping the remote host	Esta opção permite enviar um teste de “ping” aos hosts remotos em várias portas para determinar se estão “ativos”.
Netstat Portscanner (WMI)	Esta opção usa o netstat para verificar se há portas abertas no computador local. Depende da disponibilidade do comando netstat por meio de uma conexão WMI com o alvo. Esta varredura se destina a sistemas do tipo Windows e requer credenciais de autenticação.  A varredura por WMI usa o netstat para determinar portas abertas, portanto, ignora todos os intervalos de portas especificados. Se um enumerador de portas (netstat ou SNMP) for executado, o intervalo de portas torna-se “all” (todas). No entanto, o Nessus manterá a opção “consider unscanned ports as closed” (considerar portas não verificadas como fechadas) se estiver selecionada.
Nessus TCP Scanner	Usa o scanner de TCP integrado do Nessus para identificar portas TCP abertas nos alvos. Esse scanner é otimizado e possui alguns recursos de ajuste automático.  Em algumas plataformas (por exemplo, Windows e Mac OS X), a seleção do scanner fará com que o Nessus use o scanner SYN para evitar problemas graves de desempenho nativos desses sistemas operacionais.
Nessus SYN Scanner	Usa o scanner de SYN integrado do Nessus para identificar portas TCP abertas nos alvos. As varreduras SYN são um método popular para realizar varreduras de portas

e, geralmente, são consideradas um pouco menos invasivas do que as varreduras TCP. O scanner envia um pacote SYN à porta, aguarda a resposta SYN-ACK e determina o estado da porta de acordo com uma resposta ou a falta de resposta.

O menu “**Performance**” (Desempenho) possui opções que controlam o número de varreduras a ser iniciado. Essas opções podem ser as mais importantes ao configurar uma varredura, pois têm maior impacto sobre o tempo de varredura e a atividade da rede.

Opção	Descrição
Max Checks Per Host	Esta configuração limita o número máximo de verificações que um scanner Nessus realiza em um único host ao mesmo tempo.
Max Hosts Per Scan	Esta configuração limita o número máximo de hosts que um scanner Nessus pode verificar ao mesmo tempo.
Network Receive Timeout (seconds)	O valor padrão é cinco segundos. Esse é o tempo que o Nessus deve esperar por uma resposta do host, exceto se definido com outro valor por um plugin. Se a varredura for feita em uma conexão lenta, será preciso definir este valor com um número maior de segundos.
Max Simultaneous TCP Sessions Per Host	Esta configuração limita o número máximo de sessões TCP estabelecidas para um único host.  Esta opção de congestionamento de TCP também controla o número de pacotes por segundo que o scanner SYN enviará (por exemplo, se esta opção estiver definida como 15, o scanner SYN enviará 1500 pacotes por segundo, no máximo).
Max Simultaneous TCP Sessions Per Scan	Esta configuração limita o número máximo de sessões TCP estabelecidas para toda a varredura, independentemente do número de hosts verificados.  Para os scanners Nessus instalados em computadores com Windows XP, Vista e 7, este valor deve ser de no máximo 19 para se obter resultados precisos.
Reduce Parallel Connections on Congestion	Permite que o Nessus detecte o envio de um grande número de pacotes e quando o pipe da rede atingir a capacidade máxima. Se forem detectados, o Nessus reduzirá a velocidade da varredura ao nível adequado para diminuir o congestionamento. Ao diminuir o congestionamento, o Nessus tentará reutilizar o espaço disponível no pipe da rede automaticamente.
Use Kernel Congestion Detection (Linux Only)	Permite que o Nessus monitore a CPU e outros mecanismos internos em caso de congestionamento e diminua o ritmo de maneira proporcional. O Nessus tentará usar sempre o máximo de recursos disponível. Este recurso está disponível apenas para os scanners Nessus instalados em Linux.

O menu “**Advanced**” (Avançadas) define outras opções relacionadas a como a varredura deve se comportar:

Opção	Descrição
Safe Checks	A opção Safe Checks (Verificações Seguras) desativa todos os plugins que podem afetar negativamente o host remoto.

Silent Dependencies	Se esta opção for selecionada, a lista de dependências não será incluída no relatório. Se desejar incluir a lista de dependências no relatório, desmarque a caixa de seleção.
Log Scan Details to Server	Salva detalhes adicionais da varredura no registro do servidor Nessus (<code>nessusd.messages</code>), incluindo a ativação ou encerramento do plugin ou se um plugin foi interrompido. O registro resultante pode ser usado para confirmar se determinados plugins foram usados e se os hosts foram examinados.
Stop Host Scan on Disconnect	Se estiver selecionado, o Nessus cessará a varredura se detectar que o host parou de responder. Isso pode ocorrer se os usuários desligarem seus PCs durante uma varredura, se um host parar de responder depois de um plugin de negação de serviço ou se o mecanismo de segurança (por exemplo, IDS) bloqueou o tráfego para um servidor. Se as varreduras continuarem nesses computadores, o tráfego desnecessário será enviado e atrasará a verificação.
Avoid Sequential Scans	Normalmente, o Nessus verifica uma lista de endereços IP em sequência. Se a opção estiver marcada, o Nessus verificará a lista de hosts em ordem aleatória. Isto pode ser útil para ajudar a distribuir o tráfego de rede direcionado a uma sub-rede específica durante varreduras extensas.
Designate Hosts by their DNS Name	Deve-se usar o nome do host em vez do endereço IP na impressão do relatório.



O intervalo especificado para uma varredura de portas será aplicado às varreduras TCP e UDP.

Credentials (Credenciais)

A guia “**Credentials**” (Credenciais) na imagem abaixo permite configurar o scanner Nessus para o uso de credenciais de autenticação durante a varredura. A definição de credenciais permite que o Nessus realize um número maior de verificações e gere resultados de varredura mais precisos.

O item de menu suspenso “**Windows credentials**” (Credenciais do Windows) possui configurações para fornecer ao Nessus informações, como o nome da conta SMB, senha e nome do domínio. O protocolo SMB (bloqueio de mensagens do servidor) é um protocolo de compartilhamento de arquivos que permite aos computadores compartilhar informações de forma transparente através da rede. Se as informações forem fornecidas, o Nessus poderá encontrar informações locais de um host Windows remoto. Por exemplo, o uso de credenciais permite que o Nessus determine se foram aplicados patches de segurança importantes. Não é necessário modificar outros parâmetros de SMB em relação às configurações padrão.



Quando diversas contas SMB forem configuradas, o Nessus tentará fazer o login com as credenciais fornecidas em sequência. Depois de ser autenticado com um conjunto de credenciais, o Nessus irá verificar as credenciais fornecidas subsequentes, mas só irá usá-las se os privilégios administrativos forem concedidos com o acesso do usuário pré-fornecido com as contas.

Algumas versões do Windows permitem criar uma nova conta e designá-la como um “administrador”. Essas contas nem sempre são adequadas para fazer varreduras com credenciais. A Tenable recomenda que a conta administrativa original, denominada “Administrator”, seja usada para varreduras com credenciais, para garantir que o acesso integral seja permitido. Em algumas versões do Windows, essa conta pode estar oculta. A conta de administrador real pode ser reexibida executando um prompt do DOS com privilégios administrativos e digitando o seguinte comando:

```
C:\> net user administrator /active:yes
```

Se uma conta SMB de manutenção for criada com privilégios limitados de administrador, o Nessus poderá realizar varreduras em diversos domínios de maneira fácil e segura.

A Tenable recomenda que os administradores de rede criem contas específicas de domínio para facilitar os testes. O Nessus conta com diversas verificações de segurança para Windows NT, 2000, Server 2003, XP, Vista, Windows 7 e Windows 2008, que serão mais precisas se uma conta de domínio for fornecida. Na maioria dos casos, o Nessus tentará aplicar diversas verificações caso uma conta não seja fornecida.



O serviço de registro remoto do Windows permite que computadores remotos com credenciais acessem o registro do computador a ser auditado. Se o serviço não estiver em execução, não será possível ler chaves e valores do registro, **mesmo com credenciais completas**. Para obter mais informações, consulte o artigo [“Dynamic Remote Registry Auditing - Now you see it, now you don’t!”](#) no blog da Tenable. Esse serviço **deve ser iniciado** para que uma varredura com credenciais do Nessus audite integralmente um sistema usando credenciais.

Os usuários podem selecionar **“SSH settings”** (Configurações SSH) no menu suspenso e inserir credenciais para a varredura de sistemas Unix. As credenciais são usadas para obter informações locais de sistemas Unix remotos para auditoria de patches ou verificações de conformidade. Existe um campo para a inserção do nome de usuário do SSH da

conta que realizará as verificações no sistema Unix de destino, juntamente com a senha ou chave pública do SSH e um par de chaves privadas. Existe também um campo para a inserção da frase-senha da chave SSH, se necessário.



O Nessus 4 permite o uso dos algoritmos criptográficos **blowfish-cbc**, **aes-cbc** e **aes-ctr**.

As varreduras credenciadas mais eficazes são aquelas em que as credenciais fornecidas têm privilégios “root”. Uma vez que muitos locais não permitem o login remoto como root, os usuários do Nessus podem acessar “**su**” ou “**sudo**” com uma senha distinta em uma conta criada para ter os privilégios “**su**” ou “**sudo**”. Além disso, o Nessus pode atribuir privilégios em dispositivos Cisco ao selecionar “**Cisco 'enable'**”.

O Nessus pode usar o acesso por chaves SSH para se autenticar em um servidor remoto. Se um arquivo SSH **known_hosts** estiver disponível e fornecido com base na política de varredura, o Nessus tentará fazer o login apenas nos hosts deste arquivo. Além disso, a opção “Preferred SSH port” (Porta SSH preferencial) pode ser configurada para indicar ao Nessus que se conecte com o SSH se estiver funcionando em uma porta que não seja a porta 22.

O Nessus criptografa todas as senhas armazenadas nas políticas. No entanto, as boas práticas recomendam o uso de chaves SSH (e não senhas SSH) para autenticação. Isso ajuda a assegurar que o mesmo nome de usuário e senha usados para auditar os servidores SSH conhecidos não sejam usados para efetuar o login em um sistema que não esteja sob seu controle. Dessa forma, não é recomendável usar senhas SSH, a menos que seja absolutamente necessário.



O Nessus também oferece uma opção “su+sudo”, que pode ser usada caso um sistema não conceda privilégios de login remotos a contas privilegiadas.

A captura de tela a seguir mostra as opções SSH disponíveis. O menu suspenso “Elevate privileges with” (Elevar privilégios com) fornece os vários métodos de elevar os privilégios após serem autenticados.

General Settings

Credentials

Plugins

Preferences

Policy Credentials

Credential TypeSSH settings

SSH user name

root

SSH password (unsafe!)

SSH public key to use

Browse...

SSH private key to use

Browse...

Passphrase for SSH key

Elevate privileges with

Nothing

su login

Escalation account

root

Escalation password

SSH known_hosts file

Browse...

Preferred SSH port

22

Client version

OpenSSH_5.0

Se outra conta for usada além de `root` para elevação de privilégios, pode ser especificada em “**Escalation account**” (Elevação de conta) com a opção “**Escalation password**” (Senha de elevação).

“Kerberos configuration” (Configuração do Kerberos) permite especificar credenciais com o uso de chaves do Kerberos a partir de um sistema remoto:

Policy Credentials

Credential Type Kerberos configuration

Kerberos Key Distribution Center (KDC)

Kerberos KDC Port

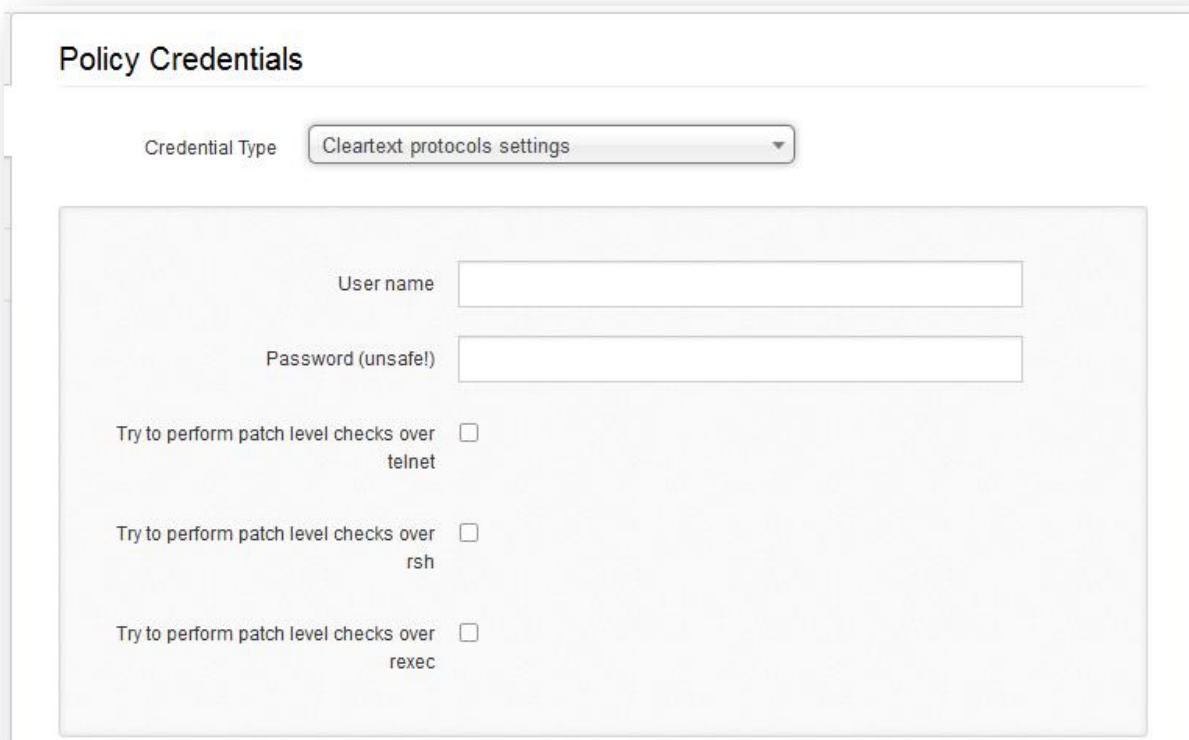
88

Kerberos KDC Transport

udp

Kerberos Realm (SSH only)

Além disso, se um método seguro de varreduras credenciadas não estiver disponível, os usuários podem forçar o Nessus a executar varreduras por meio de protocolos sem segurança ao selecionar o item “**Cleartext protocol settings**” (Configurações de protocolo de texto simples) no menu suspenso. Os protocolos de texto simples disponíveis para esta opção são **telnet**, **rsh** e **rexec**. Além disso, há caixas de seleção para forçar o Nessus a executar varreduras em nível de patch em protocolos sem segurança:



Policy Credentials

Credential Type: Cleartext protocols settings

User name:

Password (unsafe!):

Try to perform patch level checks over telnet: ☐

Try to perform patch level checks over rsh: ☐

Try to perform patch level checks over rexec: ☐

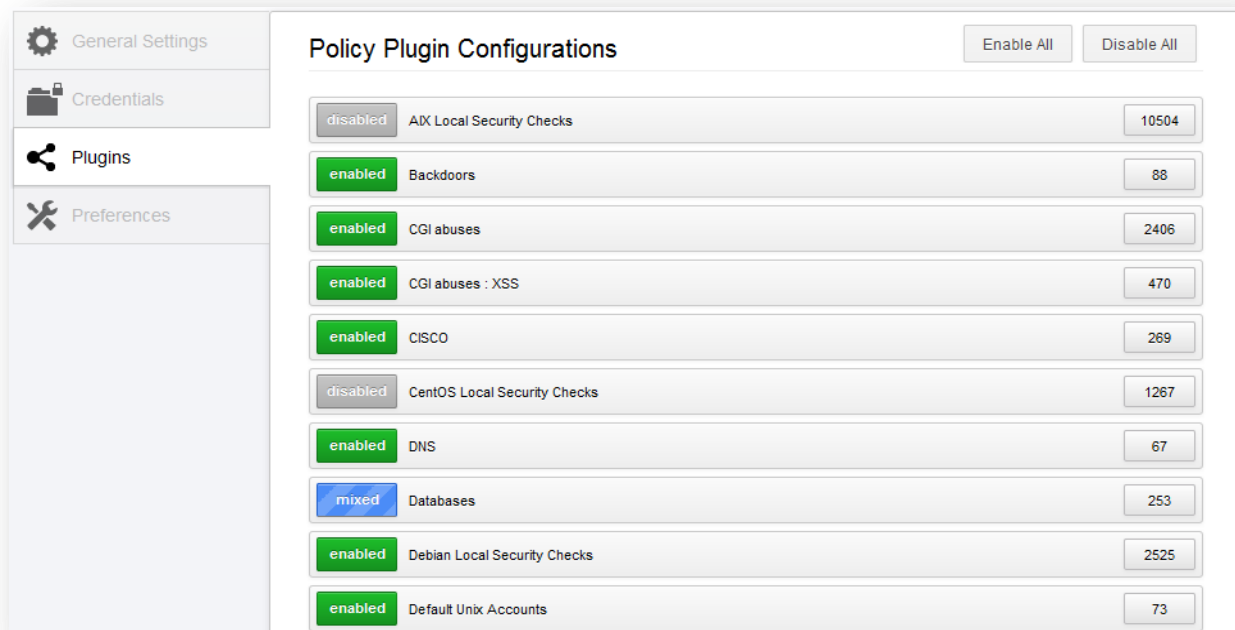
Normalmente, todas as senhas (e a própria política) são criptografadas. Se a política for salva em um arquivo **.nessus** e se o arquivo **.nessus** for posteriormente copiado em uma instalação do Nessus distinta, nenhuma senha da política poderá ser usada pelo segundo scanner Nessus, pois ele não será capaz de decodificá-la.



Não é recomendável usar credenciais em texto simples de qualquer tipo. Se as credenciais forem enviadas de maneira remota (por meio de uma varredura do Nessus, por exemplo), elas poderão ser interceptadas por qualquer pessoa com acesso à rede. Use mecanismos de autenticação criptografada sempre que possível.

Plugins

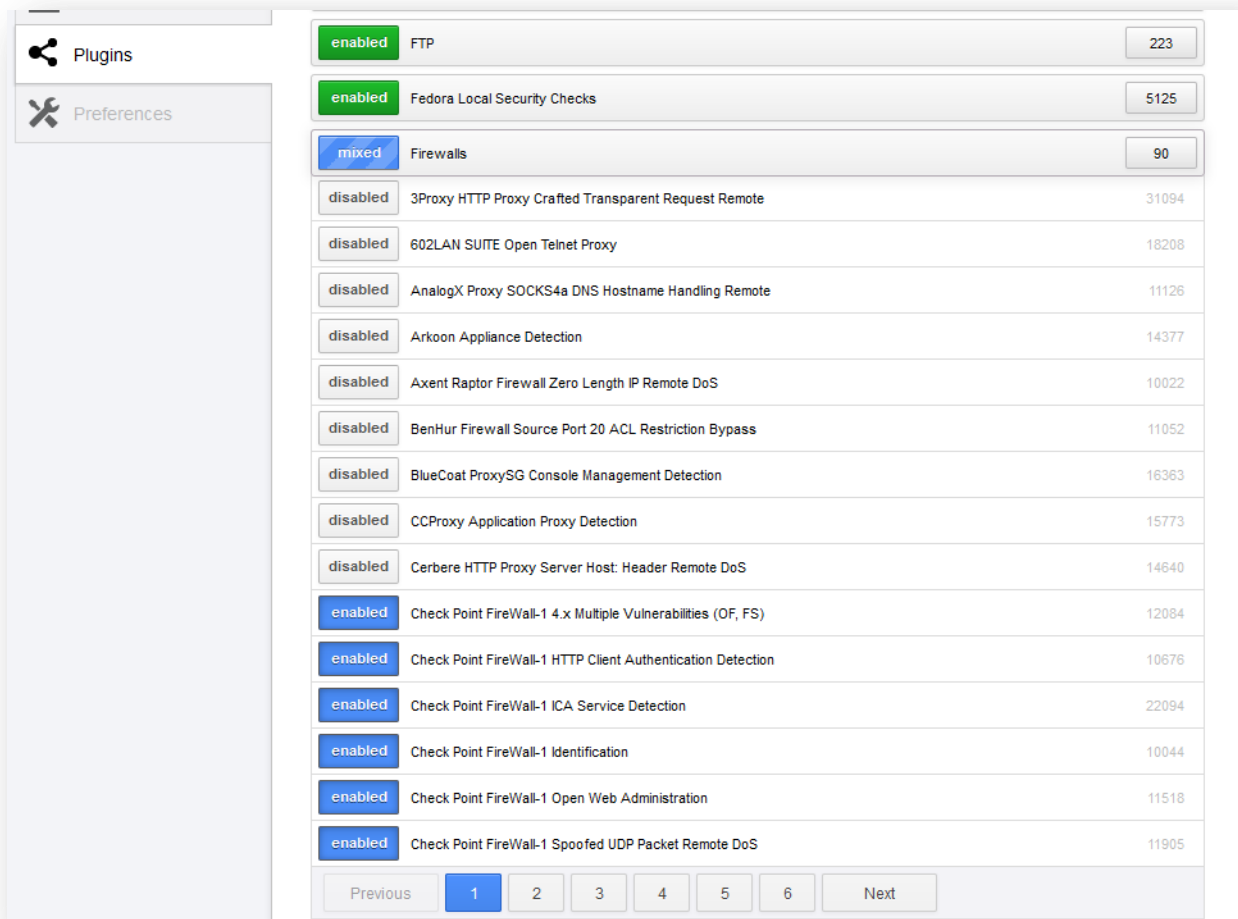
A guia **Plugin Selection** (Seleção de Plugins) permite que o usuário escolha verificações de segurança específicas por família de plugin ou verificações individuais.



The screenshot displays the 'Policy Plugin Configurations' window. On the left is a sidebar with navigation options: 'General Settings' (gear icon), 'Credentials' (key icon), 'Plugins' (network icon), and 'Preferences' (wrench icon). The main area is titled 'Policy Plugin Configurations' and includes 'Enable All' and 'Disable All' buttons. Below the title is a table of plugins with their status and counts.

Status	Plugin Name	Count
disabled	AIX Local Security Checks	10504
enabled	Backdoors	88
enabled	CGI abuses	2406
enabled	CGI abuses : XSS	470
enabled	CISCO	269
disabled	CentOS Local Security Checks	1267
enabled	DNS	67
mixed	Databases	253
enabled	Debian Local Security Checks	2525
enabled	Default Unix Accounts	73

É possível clicar em uma família de plugins para ativar (verde) ou desativar (cinza) a família inteira. A seleção da família exibirá a lista de seus plugins. Plugins individuais podem ser ativados ou desativados para criar políticas de varredura específicas. Uma família com alguns plugins desabilitados ficará azul e exibirá “mixed” (misto) para indicar que apenas alguns dos plugins estão habilitados. Clicar na família de plugins carregará a lista completa de plugins e permitirá uma seleção granular com base em suas preferências de varredura:



A seleção de um plugin específico mostrará o resultado do plugin a ser exibido como em um relatório. O resumo e a descrição fornecerão mais detalhes sobre a vulnerabilidade a ser examinada. Rolar para baixo no navegador também exibirá informações adicionais sobre soluções, referências adicionais se disponíveis, informações sobre riscos, informações sobre exploits e quaisquer referências cruzadas informativas ou de banco de dados de vulnerabilidades.

 2BGal disp_album.php id_album Parameter SQL Injection

Back

Synopsis

The remote web server contains a PHP application that is susceptible to a SQL injection attack.

Description

The remote host appears to be running 2BGal, a photo gallery software written in PHP.

There is a flaw in the 'disp_album.php' script which fails to sanitize input to the 'id_album' field. This may allow anyone to inject arbitrary SQL commands. An attacker could exploit this to obtain sensitive information and possibly gain administrative access to the remote web application.

Solution

The solution is unknown at this time.

See Also

<http://archives.neohapsis.com/archives/bugtraq/2004-12/0344.html>

Plugin Information

Plugin Type: remote

Plugin Publication Date: 2004/12/23

Plugin Last Modification Date: 2011/03/12

Risk Information

Risk Factor: High

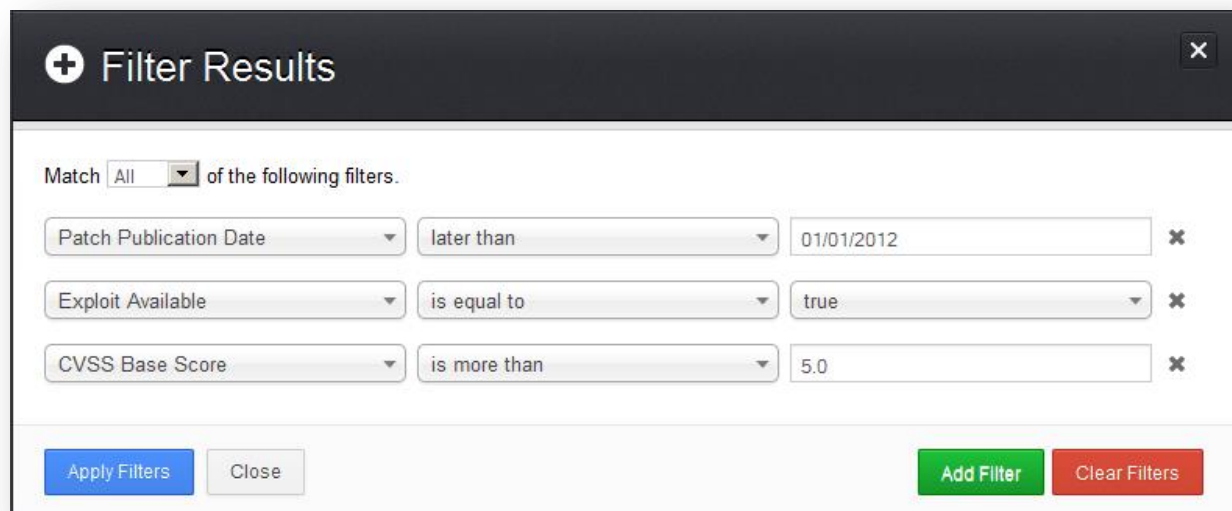
Na parte superior da página da família de plugins, é possível criar filtros para construir uma lista de plugins a serem incluídos na política. Os filtros permitem o controle granular sobre a seleção de plugins. Vários filtros podem ser definidos em uma única política. Para criar um filtro, clique no botão “**Filter Options**” (Opções de filtro):

The screenshot shows a 'Filter Results' dialog box with a dark header. Below the header, there is a section labeled 'Match' with a dropdown menu set to 'All' and the text 'of the following filters.' Below this, there is a single filter configuration row. It consists of a dropdown menu with 'Bugtraq ID' selected, followed by a dropdown menu with 'is equal to' selected, and a text input field containing 'Example: NUMBER'. To the right of the text input is a small 'x' icon. At the bottom of the dialog, there are four buttons: 'Apply Filters' (blue), 'Close' (grey), 'Add Filter' (green), and 'Clear Filters' (red).

Cada filtro criado oferece várias opções para refinar a busca. Os critérios de filtragem podem se basear em “Any” (Qualquer), em que qualquer critério retornará coincidências, ou “All” (Todos), em que todos os critérios de filtragem devem estar presentes. Por exemplo, para pesquisar uma política que inclui apenas plugins que têm um exploit associado em um quadro de exploit comercial, é possível criar três filtros e selecionar “Any” como critério:

The screenshot shows a 'Filter Results' dialog box with a dark header. Below the header, there is a section labeled 'Match' with a dropdown menu set to 'Any' and the text 'of the following filters.' Below this, there are three filter configuration rows. Each row consists of a dropdown menu with a framework name selected, followed by a dropdown menu with 'is equal to' selected, and a dropdown menu with 'true' selected. To the right of each 'true' dropdown is a small 'x' icon. At the bottom of the dialog, there are four buttons: 'Apply Filters' (blue), 'Close' (grey), 'Add Filter' (green), and 'Clear Filters' (red).

Para criar uma política que contenha plugins que correspondam a vários critérios, é possível selecionar “All” e adicionar os filtros desejados. Por exemplo, a política a seguir deve incluir qualquer plugin publicado após 1 de janeiro de 2012 com um exploit público e CVSS Base Score superior a 5.0:



+ Filter Results ×

Match **All** of the following filters.

Patch Publication Date	later than	01/01/2012	×
Exploit Available	is equal to	true	×
CVSS Base Score	is more than	5.0	×

Apply Filters **Close** **Add Filter** **Clear Filters**

Para obter uma lista completa de critérios de filtragem, consulte a seção [Report Filters](#) deste documento.



Para usar filtros para a criação de políticas, recomenda-se começar desativando todos os plugins. Usando os filtros de plugins, selecione apenas os plugins que deseja incluir na política. Depois de concluído, selecione cada família de plugins e clique em “Enable Plugins”.

Ao criar e salvar uma política, todos os plugins selecionados inicialmente são armazenados. Quando novos plugins forem recebidos com a atualização de feeds de plugins, serão ativados automaticamente se a família à qual estiverem associados for ativada. Se a família estiver desativada ou parcialmente ativada, os novos plugins da família também serão desativados automaticamente.



A família “Denial of Service” (Negação de serviço) contém alguns plugins que podem causar falhas em uma rede caso a opção “Safe Checks” (Verificações seguras) não estiver ativa, mas contém algumas verificações úteis que não causam danos. A família “Denial of Service” pode ser usada junto com “Safe Checks” para garantir que nenhum plugin potencialmente nocivo seja executado. No entanto, recomenda-se que a família “Denial of Service” não seja usada em uma rede de produção.

Preferences (Preferências)

A guia “**Preferences**” (Preferências) contém meios de controle individualizados para configuração de varreduras. Selecione um item no menu suspenso para exibir itens de configuração adicionais para a categoria selecionada. Observe que esta é uma lista dinâmica de opções de configuração e depende do feed de plugins, das políticas de auditoria e de outras funções às quais o scanner Nessus conectado tem acesso. Um scanner com ProfessionalFeed pode ter opções de configuração mais avançadas do que um scanner configurado com o HomeFeed. Esta lista também pode mudar à medida que os plugins são adicionados ou modificados.

A tabela a seguir oferece uma descrição geral de todas as preferências. Para obter informações detalhadas com relação a cada item de preferência, consulte a seção Como verificar [detalhes de preferências](#) neste documento.

Menu Preference	Descrição
ADSI settings	O Active Directory Service Interfaces obtém informações do servidor MDM (Mobile Device Management) sobre dispositivos Android e iOS.
Apple Profile Manager API Settings	Um recurso do ProfessionalFeed que habilita enumeração e varredura de vulnerabilidades para aplicativos com Apple iOS (por exemplo, iPhone, iPad).
Cisco IOS Compliance Checks	Opção de ProfessionalFeed que permite que um arquivo de política seja especificado para testar dispositivos Cisco IOS com base em padrões de conformidade.
Database Compliance Checks	Opção de ProfessionalFeed que permite que um arquivo de política seja especificado para testar bancos de dados DB2, SQL Server, MySQL e Oracle com base em padrões de conformidade.
Database Settings	Opções usadas para especificar o tipo de banco de dados a ser verificado, bem como as credenciais a serem usadas.
Do not scan fragile devices	Conjunto de opções que instrui o Nessus a não verificar dispositivos específicos devido ao risco de danificar o alvo.
Global variable settings	Grande variedade de opções de configuração para o Nessus.
HTTP cookies import	Para os testes de aplicativos da web, esta preferência especifica um arquivo externo para a importação de cookies HTTP, de modo a permitir a autenticação do aplicativo.
HTTP login page	Definições relacionadas à página de login para testes de aplicativos da Web.
IBM iSeries Compliance Checks	Opção de ProfessionalFeed que permite que um arquivo de política seja especificado para teste de sistemas IBM iSeries com base em padrões de conformidade.
IBM iSeries Credentials	Opção que especifica as credenciais para sistemas IBM iSeries.
ICCP/COTP TSAP Addressing Weakness	Uma opção ProfessionalFeed relacionada aos testes Controle de supervisão e aquisição de dados (SCADA).
Login configurations	Local em que as credenciais são especificadas para teste de serviços HTTP, NNTP, FTP, POP e IMAP básicos.
Modbus/TCP Coil Access	Uma opção ProfessionalFeed relacionada aos testes Controle de supervisão e aquisição de dados (SCADA).
Nessus SYN scanner	Opções relacionadas ao scanner SYN integrado.
Nessus TCP scanner	Opções relacionadas ao scanner TCP integrado.
News Server (NNTP) Information Disclosure	Um conjunto de opções que verifica a presença de vulnerabilidades de divulgação de informações nos servidores NNTP.
Oracle Settings	Opções relacionadas às instalações de banco de dados do Oracle.
PCI DSS compliance	Opção do ProfessionalFeed que instrui o Nessus a comparar os resultados de varredura com relação aos PCI DSS standards .
Patch Management:	Opções de integração do Nessus com o servidor de gerenciamento de patches Red

Red Hat Satellite Server Settings	Hat Satellite. Consulte o documento Patch Management Integration para obter mais informações.
Patch Management: SCCM Server Settings	Opções de integração do Nessus com o servidor de gerenciamento de patches System Center Configuration Manager (SCCM). Consulte o documento Patch Management Integration para obter mais informações.
Patch Management: VMware Go Server Settings	Opções de integração do Nessus com o servidor de gerenciamento de patches VMware Go Server (Shavlik). Consulte o documento Patch Management Integration para obter mais informações.
Patch Management: WSUS Server Settings	Opções de integração do Nessus com o servidor de gerenciamento de patches Windows Server Update Service (WSUS). Consulte o documento Patch Management Integration para obter mais informações.
Ping the remote host	Opções que permitem controlar descobertas de rede com base no ping do Nessus.
Port scanner settings	Duas opções que oferecem mais controle sobre a atividade de varredura de portas.
SMB Registry: Start the Registry Service during the scan	Instrui o Nessus a iniciar o serviço de registro SMB em hosts que não o possuem ativado.
SMB Scope	Instrui o Nessus a consultar os usuários do domínio em vez dos usuários locais.
SMB Use Domain SID to Enumerate Users	Opção que permite especificar o intervalo de SID para pesquisas SMB de usuários do domínio.
SMB Use Host SID to Enumerate Local Users	Opção que permite especificar o intervalo de SID para pesquisas SMB de usuários locais.
SMTP Settings	Opções de verificação de Simple Mail Transport Protocol (SMTP).
SNMP Settings	Informações de configuração e autenticação para Simple Network Management Protocol (SNMP).
Service Detection	Opções que permitem ao Nessus verificar os serviços baseados em SSL.
Unix Compliance Checks	Opção de ProfessionalFeed que permite que um arquivo de política seja especificado para teste de sistemas Unix com base em padrões de conformidade.
VMware SOAP API Settings	Informações de configuração e autenticação para SOAP APIs da VMware.
Wake-on-LAN	Instrui o Nessus a enviar pacotes Wake-on-LAN (WOL) antes de executar uma varredura.
Web Application Test Settings	Opções relacionadas a testes de aplicativos da Web.
Web mirroring	Detalhes de configuração que controlam o número de páginas da Web que o Nessus irá espelhar para analisar o conteúdo das vulnerabilidades.
Windows Compliance Checks	Opção de ProfessionalFeed que permite que um arquivo de política seja especificado para teste de sistemas Windows com base em padrões de conformidade.

Windows File Contents Compliance Checks

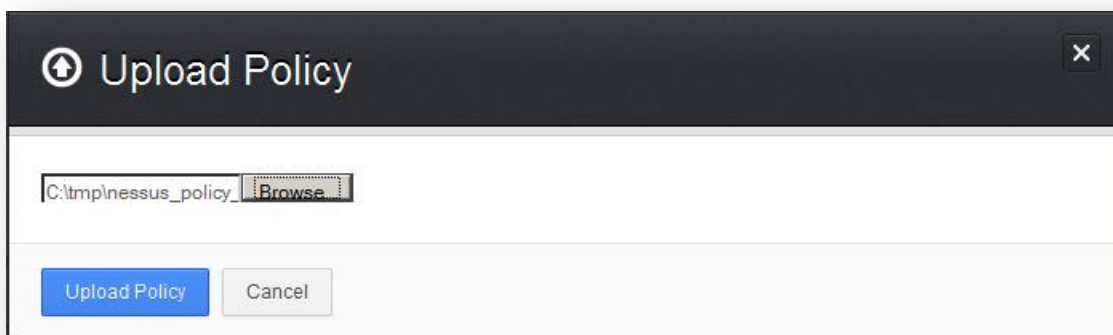
Opção de ProfessionalFeed que permite que um arquivo de política seja especificado para teste de arquivos do sistema Windows com base em padrões de conformidade.



Devido às atualizações de metadados do XML no Nessus 5, os dados de conformidade gerados com o Nessus 4 não estarão disponíveis no capítulo de verificações de conformidade dos relatórios exportados. No entanto, os dados de conformidade estarão disponíveis na interface do usuário Nessus via Web.

Importar, exportar e copiar políticas

O botão **“Upload”** (Fazer upload) na barra de menus permite enviar políticas criadas ao scanner. Na caixa de diálogo **“Browse...”** (Procurar...), selecione a política no sistema local e clique em **“Upload Policy”** (Fazer upload de política).



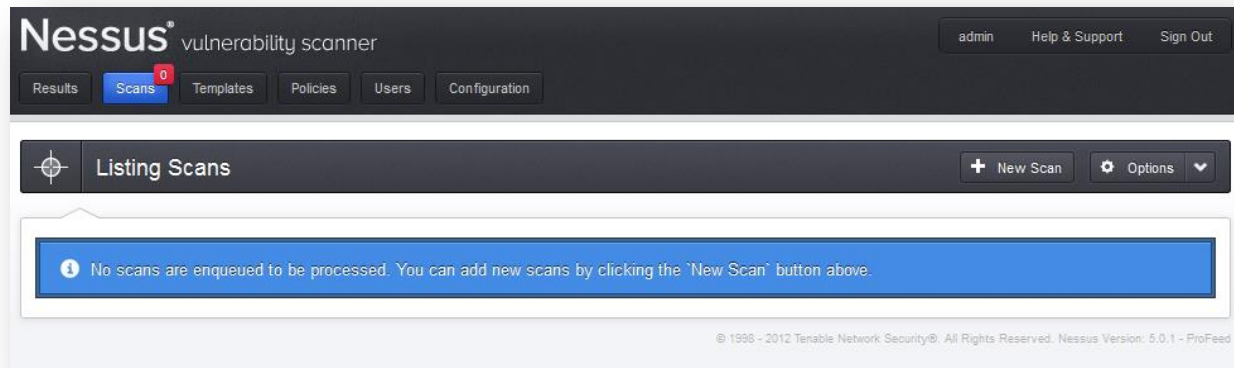
O botão **“Options”** (Opções) na barra de menus permite baixar uma política selecionada do scanner para o sistema de arquivos local. A caixa de diálogo de download do navegador permite abrir a política em um programa externo (por exemplo, editor de texto) ou salvá-la em um diretório de sua preferência.



As senhas e os arquivos **.audit** presentes em uma política **não** serão exportados.

Para criar uma política semelhante a uma política existente, mas com algumas modificações, selecione a política básica na lista e clique em **“Options”** (Opções) e, depois, em **“Copy Policy”** (Copiar política) na barra de menus. Isso criará uma cópia da política original, que pode ser editada com as modificações necessárias. Isso permite criar políticas padrão com algumas alterações necessárias para um determinado ambiente.

Criar, iniciar e programar uma varredura



Depois de criar uma política, é possível criar uma nova varredura ao clicar na opção **"Scans"** (Varreduras) na barra de menus superior e no botão **"+ New Scan"** (Nova varredura) à direita. A tela **"New Scan"** (Nova varredura) é exibida como no exemplo a seguir:

The 'New Scan' form is displayed with the following fields and options:

- Scan Title:** Text input field containing 'New Nessus Scan'.
- Scan Type:** Dropdown menu set to 'Run Now'.
- Scan Policy:** Dropdown menu set to 'Web App Tests'.
- Scan Targets:** A large text area containing the placeholder text 'Add Targets To Scan'.
- Upload Targets:** A section with a file input field and a 'Browse...' button.
- Buttons:** 'Create Scan' (blue) and 'Cancel' (grey) buttons at the bottom.

Existem cinco campos para informar o alvo da varredura:

- **Scan Title** (Título da varredura) – Define o nome que será exibido na interface do usuário Nessus para identificar a varredura.
- **Scan Type** – Selecione “Run Now” (executar imediatamente a varredura após o envio), “Scheduled” (horário em que a varredura deve começar) ou “Template” (salvar como modelo para varreduras recorrentes).
- **Scan Policy** (Política de varredura) – Selecione uma política já criada a ser usada pela varredura para definir os parâmetros que controlam o comportamento de varredura do servidor Nessus.
- **Scan Targets** – Os alvos podem ser inseridos com um endereço IP simples (por exemplo, 192.168.0.1), um intervalo de IPs (por exemplo, 192.168.0.1-192.168.0.255), uma sub-rede com a notação CIDR (por exemplo, 192.168.0.0/24) ou um host conversível (por exemplo, www.nessus.org).
- **Upload Targets** (Upload de destinos) – É possível importar um arquivo de texto com uma lista de hosts ao clicar em “Browse...” (Procurar) e selecionar um arquivo no computador local.



O arquivo de host deve ser formatado como texto ASCII, com um host por linha e sem espaços ou linhas extras. A codificação Unicode/UTF-8 não é reconhecida.

Exemplo de formatos de arquivos de host:

Hosts individuais:

```
192.168.0.100
192.168.0.101
192.168.0.102
```

Intervalo de hosts:

```
192.168.0.100-192.168.0.102
```

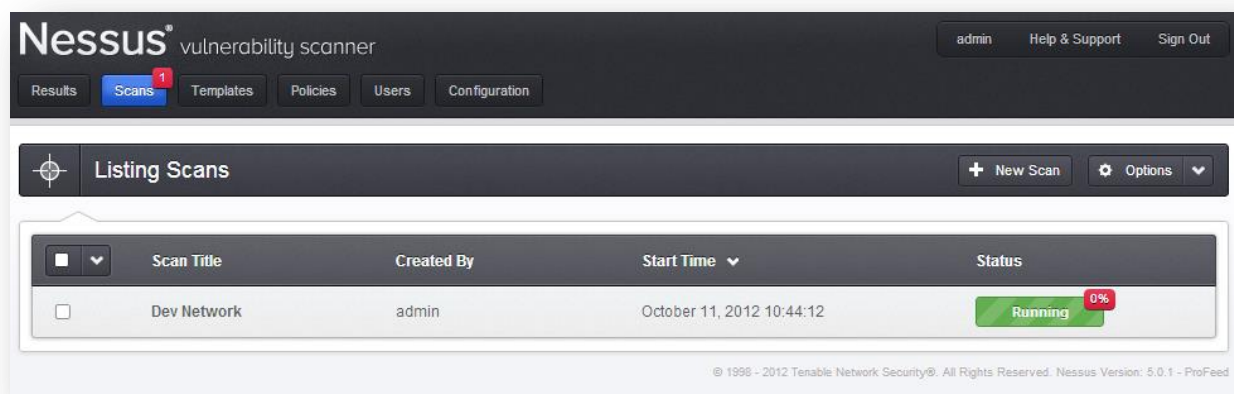
Bloco CIDR de hosts:

```
192.168.0.1/24
```

Servidores virtuais:

```
www.tenable.com[192.168.1.1]
www.nessus.org[192.168.1.1]
www.tenablesecurity.com[192.168.1.1]
```

Depois de inserir as informações de varredura, clique em “**Create Scan**” (Criar varredura). Depois do envio, a varredura iniciará imediatamente (se “Run Now” for selecionado) antes que a tela retorne à página geral de “**Scans**” (Varreduras). A barra de menus superior também atualizará o número sobreposto ao botão “**Scans**” (Varreduras) para indicar quantas varreduras estão em execução atualmente.



Depois que a varredura for iniciada, a lista Scans exibirá todas as varreduras em execução ou em pausa, além de informações básicas sobre a varredura. Depois de selecionar uma varredura específica na lista, o botão **“Options”** (Opções) no canto superior direito permite **“Pause”** (Pausar), **“Resume”** (Continuar) ou **“Stop”** (Parar) a varredura.

Quando for concluída por qualquer motivo, a varredura será retirada da lista **“Scans”** e estará disponível para revisão na guia **“Results”** (Resultados).

Se uma nova varredura estiver designada como **“Scheduled”** (Programada), uma opção será exibida para definir o horário inicial desejado e a frequência:

No menu suspenso **“Repeat”** (Repetir), a varredura pode ser programada para ser executada uma única vez, diariamente, semanalmente, mensalmente ou anualmente. Essa opção também pode ser especificada para iniciar em uma data e horário específicos. Após salvar a varredura, o Nessus iniciará a varredura no horário especificado.

+

New Scan

×

Scan Title

New Nessus Scan

Scan Type

Scheduled

Repeat

Weekly

Starts On

10/11/2012

10:00

Bahia Standard Time

Repeat Every

1 Weeks

Repeat On

☐ S
☒ M
☐ T
☒ W
☐ T
☒ F
☐ S

Scan Policy

Internal Network Scan

Scan Targets

Add Targets To Scan



As varreduras programadas estão disponíveis apenas para os clientes do ProfessionalFeed.

Se uma nova varredura for salva como um modelo, aparecerá na guia “Templates” (Modelos) à direita da guia “Scans” (Varreduras) na barra de menus. Na guia “Templates” (Modelos), os usuários podem editar, excluir ou iniciar varreduras definidas como modelo.

Nessus

vulnerability scanner

admin Help & Support Sign Out

Results

Scans

Templates

Policies

Users

Configuration

Listing Scan Templates

+ New Scan

Options

Filter Templates

	Template Title	Created By	Policy
☐	HR Internal	admin	Internal Network Scan
☐	Tenable Laptop	admin	Windows - Tenable Laptop
☐	Windows - Main Comp	admin	Windows - Main Comp (.12)
☐	Windows - Media Comp	admin	Windows - Media Comp (.20)

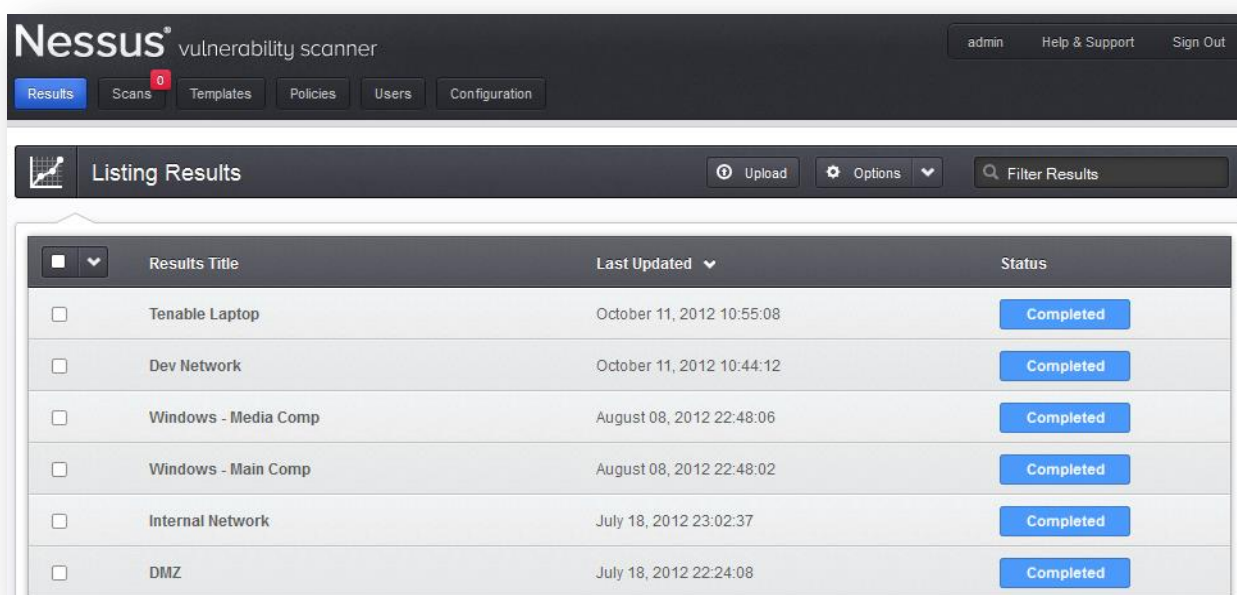
© 1998 - 2012 Tenable Network Security®. All Rights Reserved. Nessus Version: 5.0.1 - ProFeed

A mesma funcionalidade para criação de uma nova varredura pode ser acessada nessa guia. Além disso, uma caixa de entrada de filtro permite filtrar os modelos com base no campo de título. A exclusão de texto digitado nessa caixa redefinirá o filtro e exibirá todos os modelos.

Results (Resultados)

Com o lançamento do Nessus 5, os usuários podem criar seu próprio relatório por capítulos: Vulnerability Centric, Host Centric, Compliance ou Compliance Executive. O formato HTML ainda é o padrão. No entanto, se o Java estiver instalado no host do scanner, também é possível exportar relatórios em PDF. Com o uso de filtros de relatório e os recursos de exportação, os usuários podem criar relatórios dinâmicos à sua própria escolha em vez de selecioná-los em uma lista específica.

Ao clicar no guia “**Results**” (Resultados) na barra de menus superior da interface, a lista de varreduras em execução e concluídas será exibida:

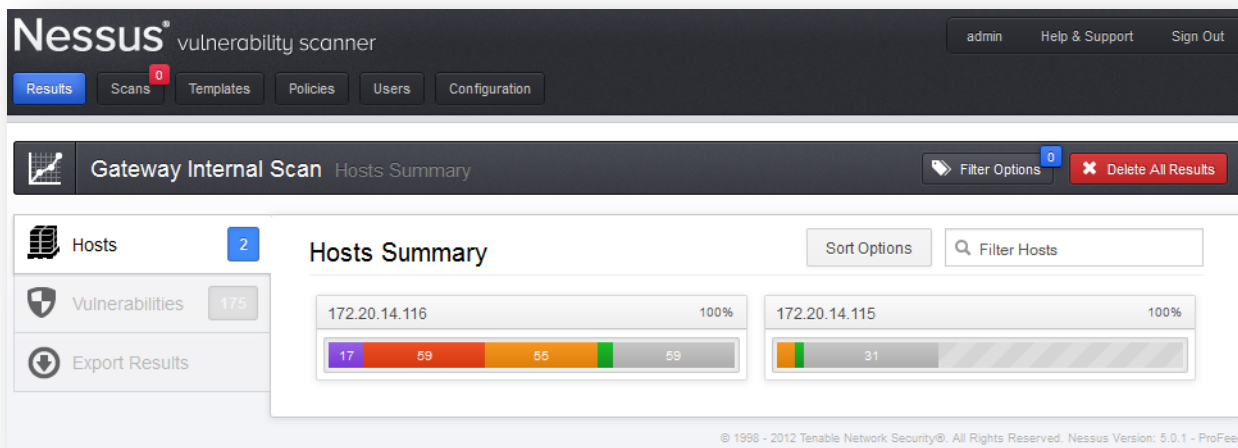


Nessus [®] vulnerability scanner			
admin	Help & Support	Sign Out	
Results	Scans	Templates	Policies
Users	Configuration		
Listing Results			
Upload		Options	
Filter Results			
☐	Results Title	Last Updated	Status
☐	Tenable Laptop	October 11, 2012 10:55:08	Completed
☐	Dev Network	October 11, 2012 10:44:12	Completed
☐	Windows - Media Comp	August 08, 2012 22:48:06	Completed
☐	Windows - Main Comp	August 08, 2012 22:48:02	Completed
☐	Internal Network	July 18, 2012 23:02:37	Completed
☐	DMZ	July 18, 2012 22:24:08	Completed

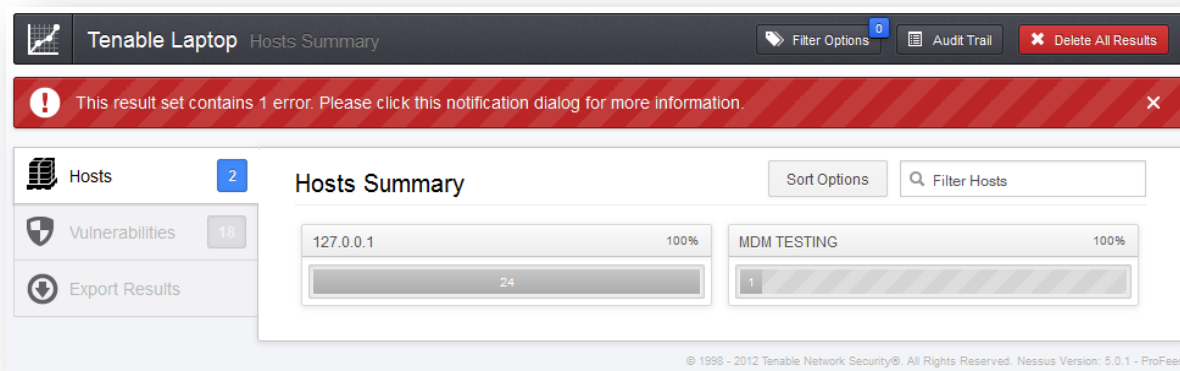
A tela “**Results**” (Resultados) funciona como um ponto central para exibir, comparar, enviar e baixar resultados de varreduras.

Procurar resultados de varreduras

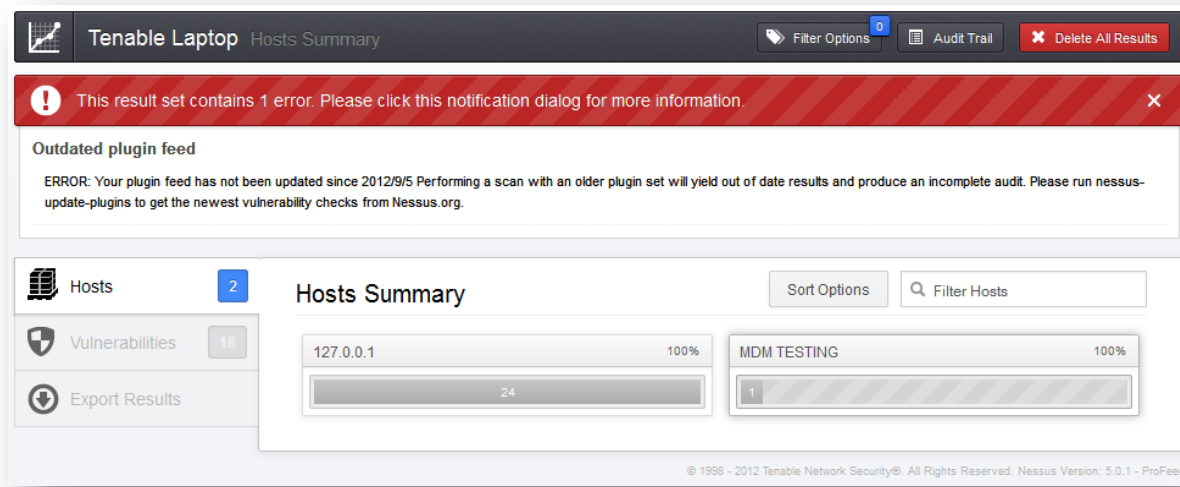
Para procurar os resultados de uma varredura, clique em um relatório na lista “**Results**” (Resultados). Isso permite exibir os resultados ao navegar pelas vulnerabilidades ou hosts, exibir portas e informações de vulnerabilidades específicas. A exibição/guia padrão é por resumo de host, que exibe uma lista de hosts com um resumo de vulnerabilidades codificado por cores para cada host:



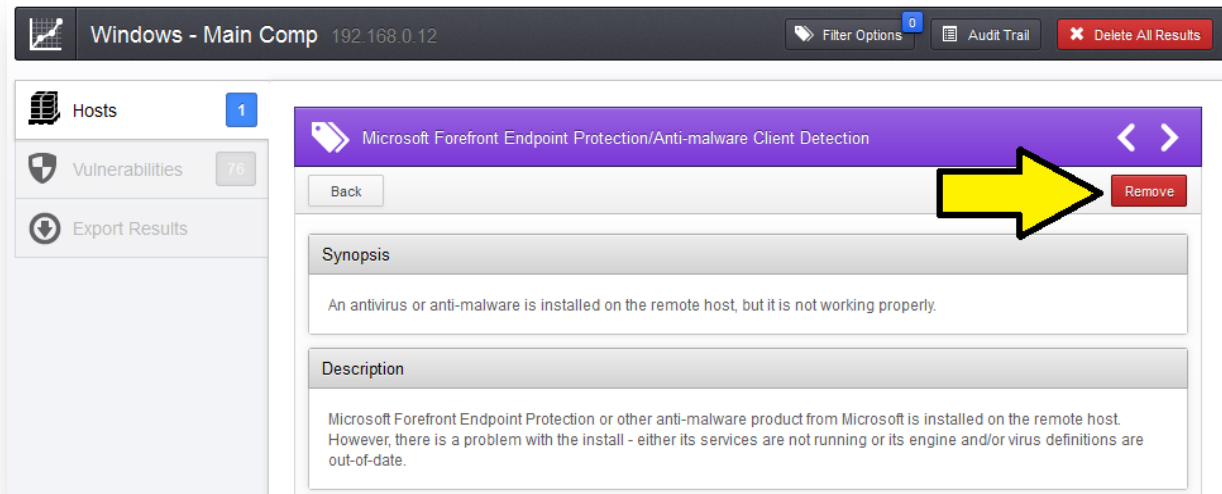
Se ocorrer algum erro durante a varredura, haverá uma notação no início dos resultados.



Clique no erro para obter mais informações:



Clicar em um host exibirá o “**Vulnerability Summary**” (Resumo de vulnerabilidades). O usuário pode exibir seletivamente informações detalhadas de vulnerabilidades a partir do relatório, incluindo sinopse, descrição, solução, referências, informações de riscos e atualizações de plugins. No canto superior direito, “**Remove**” (Remover) pode ser usada para excluir a vulnerabilidade exibida:



Tenha cuidado para selecionar “**Remove**” (Remover) logo acima da vulnerabilidade, em vez de “**Delete All Results**” (Excluir todos os resultados) na barra de menus Results (Resultados). Usando os botões de seta na barra de títulos de vulnerabilidades, você pode navegar nos resultados individualmente.

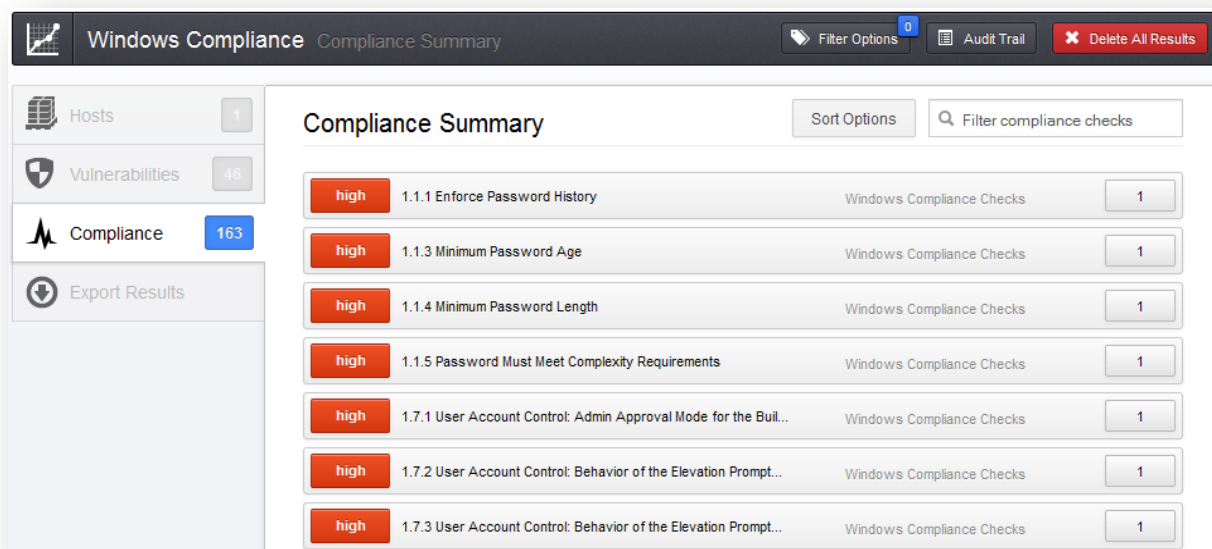
Selecionar a guia “Vulnerabilities” (Vulnerabilidades) à esquerda mudará para a Exibição de vulnerabilidades. Isso classificará os resultados por vulnerabilidades, não por hosts. Selecionar uma vulnerabilidade fornecerá as mesmas informações que antes, mas incluirá também uma lista dos hosts afetados na parte inferior.

The screenshot displays a web-based interface for a vulnerability scanner. On the left, a sidebar contains three main sections: 'Hosts' with a count of 3, 'Vulnerabilities' with a count of 13, and 'Export Results'. The main content area is titled 'Microsoft Windows SMB Service Detection' and includes a 'Back' button and a red 'Remove' button. The details are organized into several sections: 'Synopsis' (A file / print sharing service is listening on the remote host.), 'Description' (The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.), 'Solution' (n/a), 'Plugin Information' (Plugin Type: remote, Plugin Publication Date: 2002/06/05, Plugin Last Modification Date: 2012/01/31), 'Risk Information' (Risk Factor: None), and 'Affected Host List (3)'. The host list contains three entries, each with an IP address and a count of 2 in a blue box.

Affected Host List (3)	
192.168.0.30	2
192.168.0.20	2
192.168.0.12	2

Clicar em um host afetado na parte inferior carregará a exibição baseada em hosts das vulnerabilidades.

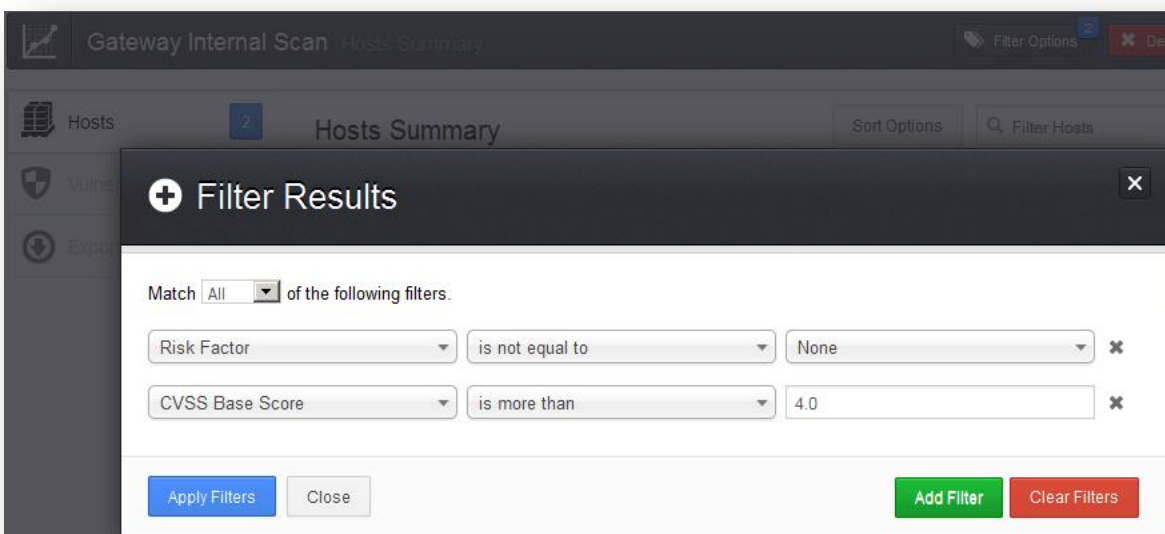
Se for iniciada uma varredura que utiliza uma [compliance policy](#), os resultados estarão em uma nova guia lateral sob o relatório da varredura, denominada “**Compliance**” (Conformidade):



Filtros de relatórios

A Nessus oferece um sistema de filtros flexível para auxiliar na exibição de resultados específicos do relatório. Os filtros podem ser usados para exibir os resultados de acordo com qualquer aspecto dos resultados de vulnerabilidades. Quando vários filtros forem usados, é possível criar exibições mais detalhadas e personalizadas dos relatórios.

Para criar um filtro, comece clicando em “**Filter Options**” (Opções de filtro) acima dos resultados de relatórios. Os filtros podem ser criados a partir de qualquer guia de relatório. Vários filtros podem ser criados com lógica que permite a filtragem complexa. Um filtro é criado ao selecionar o atributo de plugin, argumento de filtro e um valor de filtragem. Ao selecionar diversos filtros, a palavra-chave “Any” ou “All” deve ser especificada corretamente. Se “All” for selecionado, todos os resultados correspondentes aos filtros **all** (todos) serão exibidos:



Depois de ter sido definido, o filtro pode ser removido individualmente ao clicar em ✖ à direita. Além disso, todos os filtros podem ser removidos ao mesmo tempo ao selecionar “Clear Filters”. Os filtros de relatório aceitam uma grande variedade de critérios para controle granular dos resultados:

Opção	Descrição
Plugin ID (ID do plugin)	Filtra os resultados se as opções de Plugin ID forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, 42111).
Plugin Description (Descrição do plugin)	Filtra os resultados se as opções de Plugin Description forem “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “remote”).
Plugin Name (Nome do plugin)	Filtra os resultados se as opções de Plugin Name forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “windows”).
Plugin Family (Família de plugins)	Filtra os resultados se as opções de Plugin Name forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente) para as famílias de plugin do Nessus designadas. As correspondências possíveis estão disponíveis no menu suspenso.
Plugin Output (Saída de plugin)	Filtra os resultados se as opções de Plugin Description forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “PHP”).
Plugin Type (Tipo de plugin)	Filtra os resultados se as opções de Plugin Type forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente) para um dos dois tipos de plugins: local ou remoto.
Solution (Solução)	Filtra os resultados se as opções de Plugin Solution forem “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “upgrade”).
Synopsis (Sinopse)	Filtra os resultados se as opções de Solution forem “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “PHP”).
Hostname (Nome do host)	Filtra os resultados se as opções de host forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “192.168” ou “lab”).
Port (Porta)	Filtra os resultados se as opções de porta forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “80”).
Protocol (Protocolo)	Filtra os resultados se as opções de protocolo forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente) para um determinado string (por exemplo, “http”).
CPE	Filtra os resultados se as opções de Common Platform Enumeration (CPE) forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “solaris”).
CVSS Base Score	Filtra os resultados com base nas opções de CVSS base score : “ <i>is less than</i> ” (menor que), “ <i>is more than</i> ” (maior que), “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “5”).



Este filtro pode ser usado para selecionar o nível de risco. As classificações de gravidade são derivadas da respectiva pontuação CVSS, em que 0 é “Info”, inferior a 4 é “Low” (baixo), inferior a 7 é “Medium” (médio), inferior a 10 é “High” (alto) e uma pontuação CVSS igual a 10 será indicada como “Critical” (grave).

CVSS Temporal Score	Filtra os resultados se as opções de CVSS temporal score forem “ <i>is less than</i> ” (menor que), “ <i>is more than</i> ” (maior que), “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “3.3”).
CVSS Temporal Vector	Filtra os resultados se as opções de CVSS temporal vector forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “E:F”).
CVSS Vector	Filtra os resultados se as opções de CVSS vector forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “AV:N”).
Data de publicação da vulnerabilidade	Filtra os resultados com base na data de publicação da vulnerabilidade “ <i>earlier than</i> ” (inferior a), “ <i>later than</i> ” (superior a), “ <i>on</i> ” (em), “ <i>not on</i> ” (não em), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “01/01/2012”). Nota: O pressionamento do botão  próximo à data abrirá a interface do calendário para facilitar a escolha da data.
Data de publicação do patch	Filtra os resultados com base na data de publicação do plugin do Nessus com as opções “ <i>is less than</i> ” (menor que), “ <i>is more than</i> ” (maior que), “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “06/03/2011”).
Data de publicação do plugin	Filtra os resultados com base na data de publicação do plugin do Nessus com as opções “ <i>is less than</i> ” (menor que), “ <i>is more than</i> ” (maior que), “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “06/03/2011”).
Data de modificação do plugin	Filtra os resultados com base na data de modificação do plugin do Nessus com as opções “ <i>is less than</i> ” (menor que), “ <i>is more than</i> ” (maior que), “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “02/14/2010”).
CVE	Filtra os resultados se as opções de CVE reference forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “2011-0123”).
Bugtraq ID	Filtra os resultados se as opções de Bugtraq ID forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “51300”).
CERT Advisory ID	Filtra os resultados se as opções de CERT Advisory ID (também chamado de Technical Cyber Security Alert) forem “ <i>is equal to</i> ” (igual a), “ <i>is not equal to</i> ” (diferente), “ <i>contains</i> ” (contém) ou “ <i>does not contain</i> ” (não contém) para um determinado string (por exemplo, “TA12-010A”).

OSVDB ID	Filtra os resultados se as opções da ID de Open Source Vulnerability Database (OSVDB) forem “is equal to” (igual a), “is not equal to” (diferente), “contains” (contém) ou “does not contain” (não contém) para um determinado string (por exemplo, “78300”).
Secunia ID	Filtra os resultados as opções de Secunia ID forem “is equal to” (igual a), “is not equal to” (diferente), “contains” (contém) ou “does not contain” (não contém) para um determinado string (por exemplo, “47650”).
Exploit Database ID	Filtra os resultados se as opções da referência de Exploit Database ID (EBD-ID) forem “is equal to” (igual a), “is not equal to” (diferente), “contains” (contém) ou “does not contain” (não contém) para um determinado string (por exemplo, “18380”).
Metasploit Name (Nome do metasploit)	Filtra os resultados se as opções de Metasploit name forem “is equal to” (igual a), “is not equal to” (diferente), “contains” (contém) ou “does not contain” (não contém) para um determinado string (por exemplo, “xslt_password_reset”).
Exploit Hub (Concentração de exploit)	Filtra os resultados se o exploit de ExploitHub for “true” (verdadeiro) ou “false” (falso).
IAVA	Filtra os resultados se as opções da referência de IAVA forem “is equal to” (igual a), “is not equal to” (diferente), “contains” (contém) ou “does not contain” (não contém) para um determinado string (por exemplo, 2012-A-0008).
See Also (Ver também)	Filtra os resultados se as opções da referência “see also” (ver também) de plugins do Nessus forem “is equal to” (igual a), “is not equal to” (diferente), “contains” (contém) ou “does not contain” (não contém) para um determinado string (por exemplo, “seclists.org”).
Exploits Available (Exploits disponíveis)	Filtra os resultados se a vulnerabilidade tiver uma exploração pública conhecida.
Exploitability Ease (Facilidade de exploração)	Filtra os resultados se as opções de facilidade de exploração forem “is equal to” (igual a), “is not equal to” (diferente) para os seguintes valores: Exploits are available” (exploits disponíveis), “No exploit is required” (não requer exploits) ou “No known exploits are available” (nenhum exploit disponível).
Metasploit Exploit Framework (Quadro Metasploit Exploit)	Filtra os resultados com base na presença de uma vulnerabilidade no quadro Exploit Metasploit “is equal to” (igual a) verdadeira ou falsa.

Quando um filtro é usado, é possível delimitar o string ou o valor numérico por vírgulas para filtrar com base em vários strings. Por exemplo, para filtrar os resultados de maneira a exibir apenas os servidores da Web, é preciso criar um filtro “Ports”, selecionar “is equal to” e inserir “80,443,8000,8080”. Isto exibirá os resultados associados a essas quatro portas.



Os critérios de filtragem não distinguem maiúsculas e minúsculas.

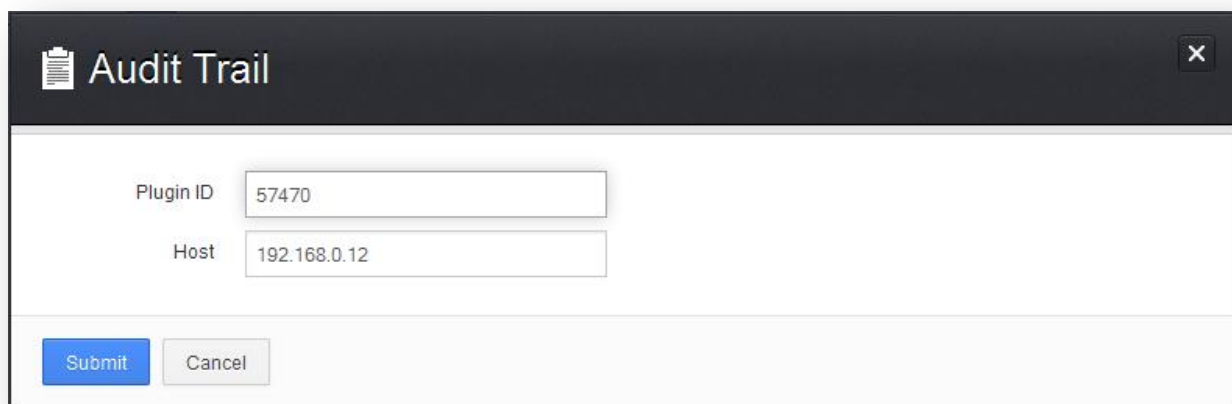
Se uma opção de filtro não estiver disponível, isso significa que o relatório não contém nenhuma opção que corresponde aos critérios. Por exemplo, se “Microsoft Bulletin” não estiver na listagem de filtros, nenhuma vulnerabilidade referente a um boletim da Microsoft foi encontrada.

Quando um filtro é criado, os resultados da varredura são atualizados para refletir os novos critérios de filtragem depois de selecionar “**Apply Filters**” (Aplicar filtros).

Depois que os resultados forem filtrados para gerar o conjunto de dados desejado, clique em “**Export Results**” (Exportar resultados) para exportar apenas os resultados filtrados. Para receber um relatório com todos os resultados, remova todos os filtros e use o recurso de exportação.

Os resultados de varredura do Nessus fornecem uma lista concisa dos plugins detectados com problemas no host. No entanto, às vezes é necessário saber porque um plugin não enviou resultados. A funcionalidade “Audit Trail” fornecerá essas informações. Comece clicando em “Audit Trail” (Trilha de auditoria) no alto.

Isto abrirá a caixa de diálogo Audit Trail. Digite a ID do plugin do qual deseja obter mais informações. Clique no botão “Submit” (Enviar) para exibir uma série ou lista de hosts relativos à consulta. Opcionalmente, é possível fornecer um IP do host para a consulta inicial para limitar os resultados de um destino de interesse. Quando o(s) host(s) for(em) exibido(s), clique em um host para exibir informações sobre a causa da falha do plugin:

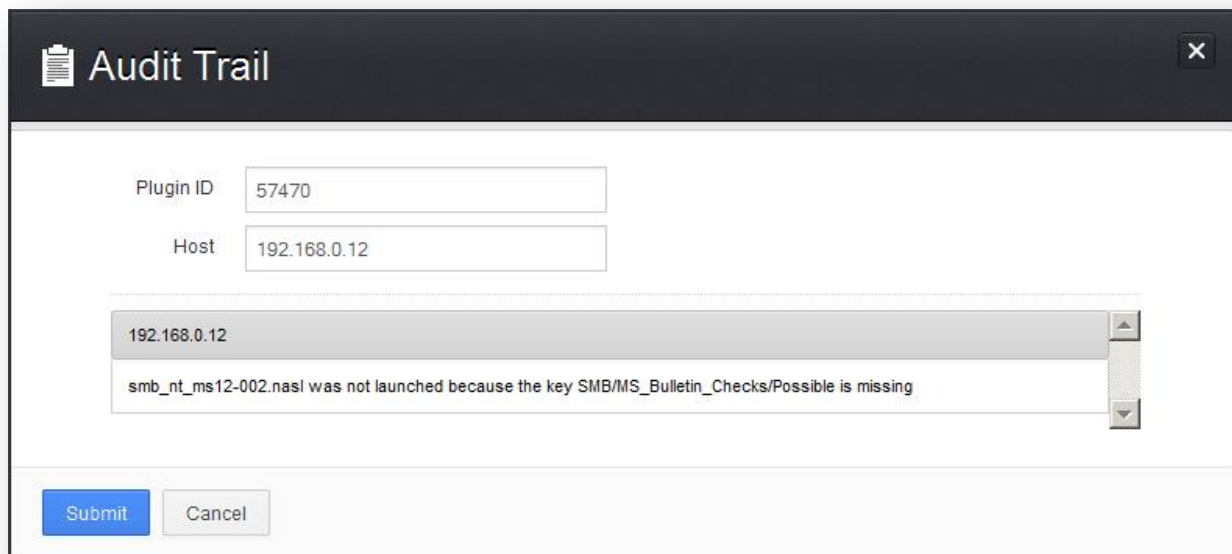


Audit Trail

Plugin ID: 57470

Host: 192.168.0.12

Submit Cancel



Audit Trail

Plugin ID: 57470

Host: 192.168.0.12

192.168.0.12

smb_nt_ms12-002.nasl was not launched because the key SMB/MS_Bulletin_Checks/Possible is missing

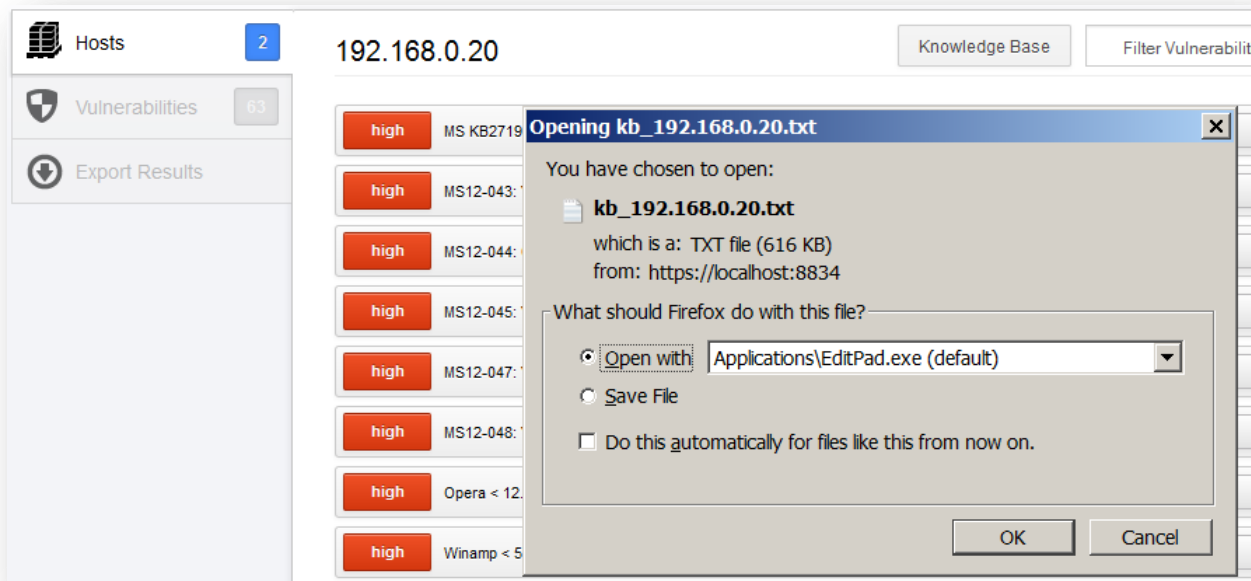
Submit Cancel



Devido aos recursos necessários para a trilha de auditoria, em alguns casos, apenas uma trilha de auditoria parcial será fornecida. A trilha de auditoria completa está disponível para um único host verificado. Se entre 2 e 512 hosts forem verificados, uma trilha de auditoria completa estará disponível somente se o servidor Nessus tiver mais de uma CPU e 2G de memória RAM. A varredura superior a 512 hosts sempre resultará em uma trilha de auditoria parcial.

Com o Nessus 5, uma Base de Conhecimento (KB) é salva com cada varredura realizada. Este é um arquivo de texto ASCII que contém um registro de informações correspondentes para a varredura realizada e os resultados encontrados. Uma base de conhecimento é normalmente útil nos casos em que é necessário suporte da Tenable, uma vez que permite que a equipe de suporte entenda exatamente o comportamento do Nessus e as informações encontradas.

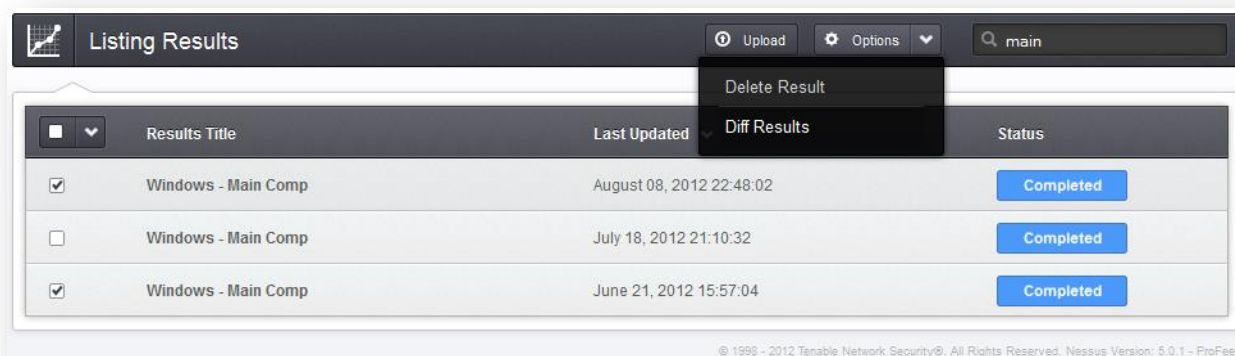
Para fazer download de uma KB, selecione um relatório e, depois, um host específico. À direita do nome do host ou IP, há um botão intitulado “Knowledge Base” (Base de conhecimento). Clique nele para fazer download da KB:



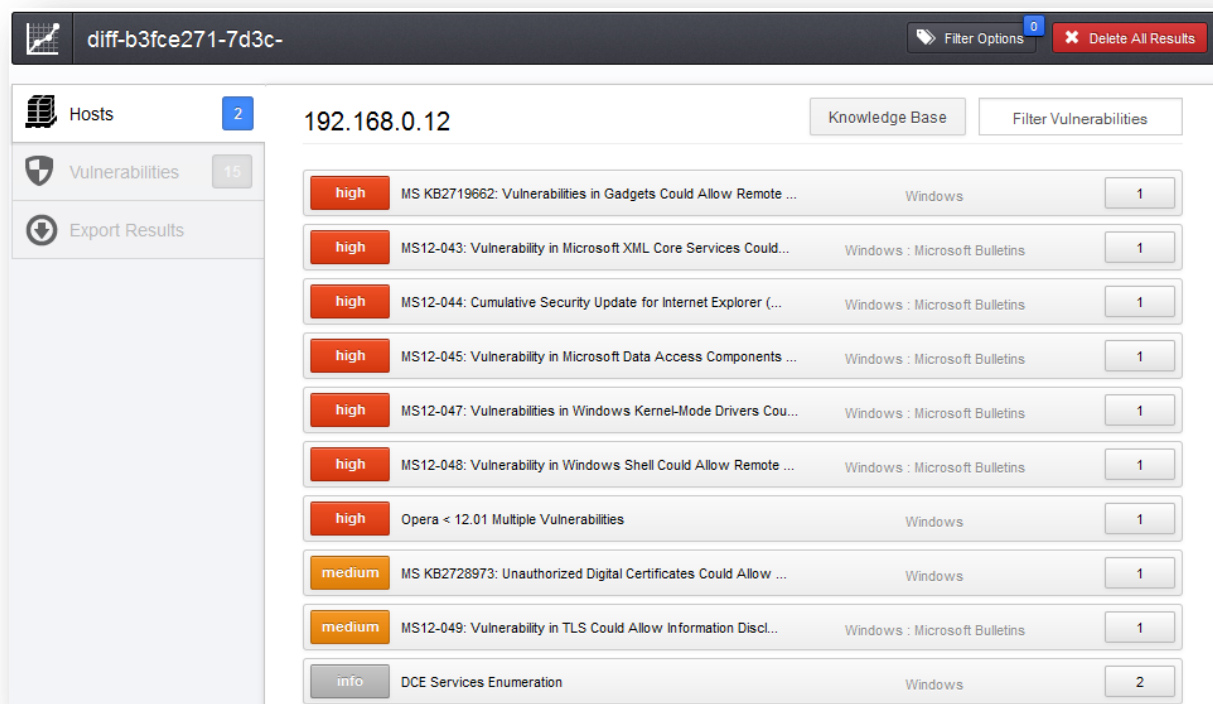
Comparar (diferenciar resultados)

Com o Nessus, é possível comparar dois relatórios de varredura para exibir as diferenças. A capacidade de exibir as diferenças de varredura ajuda a indicar as mudanças de um determinado sistema ou rede ao longo do tempo. Isto permite analisar a conformidade ao mostrar como as vulnerabilidades são corrigidas, se os sistemas recebem correções à medida que novas vulnerabilidades são encontradas ou se duas varreduras estão direcionadas aos mesmos hosts.

Para comparar relatórios, selecione duas varreduras na lista “**Results**” (Resultados), clique em “**Options**” (Opções) e selecione “**Diff Results**” (Diferenciar resultados) no menu suspenso:



O Nessus irá comparar o primeiro relatório selecionado com o segundo e produzir uma lista de resultados diferentes do primeiro. O recurso de comparação mostra o que há de novo na linha de base (ou seja, o primeiro relatório selecionado), mas não produz um diferencial de dois relatórios. A comparação destaca as vulnerabilidades descobertas e corrigidas entre as duas varreduras. No exemplo acima, “Windows – Main Comp” é uma varredura autenticada de um único host Microsoft Windows, executada várias vezes. O recurso “Compare” (Comparar) exibe as diferenças, destacando vulnerabilidades que não foram examinadas em 21 de junho:

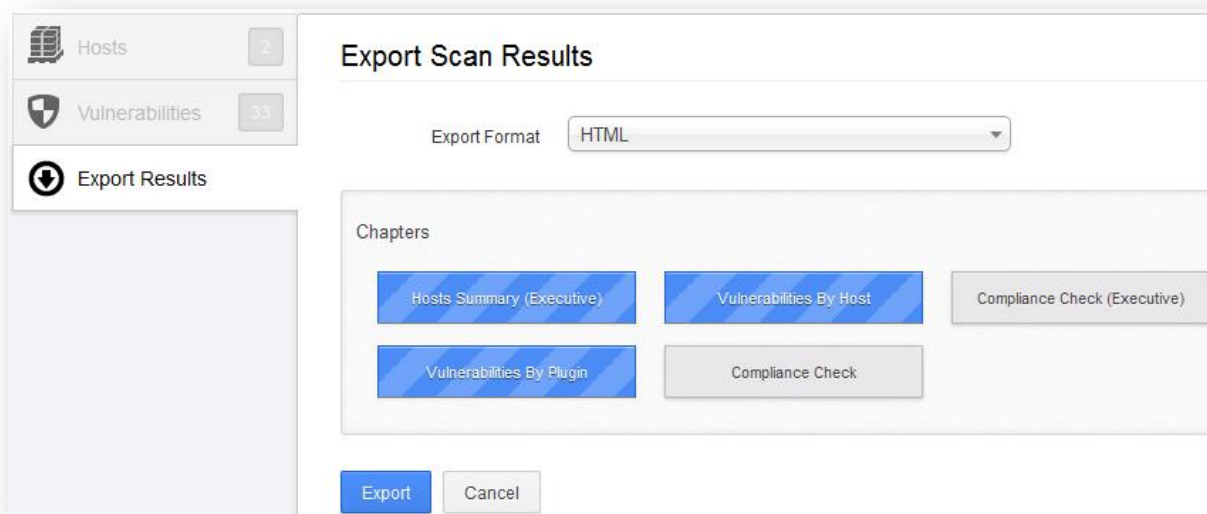


A função “Compare” está disponível apenas para os usuários do ProfessionalFeed.

Upload e download (exportar)

Os resultados das varreduras podem ser exportados de um scanner Nessus e importados para outro scanner Nessus. Os recursos “**Upload**” e “**Download**” facilitam o gerenciamento das varreduras, comparação de relatórios, backup de relatórios e a comunicação entre grupos ou organizações em uma empresa.

Para exportar uma varredura, selecione o relatório na tela “**Results**” (Resultados), selecione a guia “**Export Results**” (Exportar resultados), escolha as opções desejadas e clique em “**Export**” (Exportar). As opções especificam o formato desejado, bem como informações específicas (divididas em “capítulos”) que devem ser incluídas. Clicar no capítulo desejado destaca-o em azul para indicar que será incluído no relatório:



As varreduras de conformidade realizadas com o Nessus 5 podem ser exportadas para os formatos PDF ou HTML com os capítulos de conformidade. As varreduras importadas de versões anteriores do Nessus não serão exportadas desta maneira.

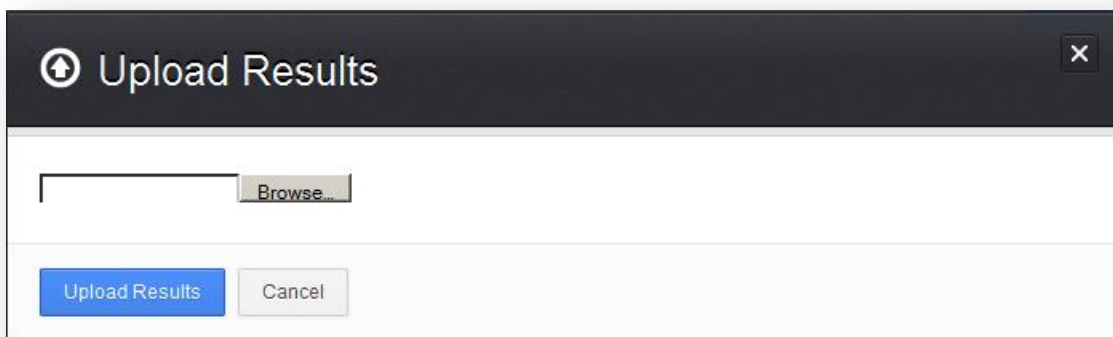
Os relatórios podem ser baixados em vários formatos. Observe que alguns formatos não permitirão a seleção de capítulos ou incluirão todas as informações.

Opção	Descrição
.nessus	Um formato do tipo XML, padrão do Nessus 4.2 e versões posteriores. Este formato usa um conjunto extenso de tags XML, que tornam a extração e a análise de informações mais granular. Este relatório não permite selecionar o capítulo.
.nessus (v1)	Um formato do tipo XML usado do Nessus 3.2 ao 4.0.2, compatível com o Nessus 4.x e Security Center 3. Este relatório não permite selecionar o capítulo.
HTML	Relatório gerado em HTML padrão, que permite selecionar o capítulo. Este relatório será aberto em uma nova guia do navegador.
PDF	Relatório gerado no formato PDF, que permite selecionar o capítulo. Dependendo do tamanho do relatório, a geração de PDF pode levar vários minutos.

	 O Oracle Java (conhecido como Java da Sun Microsystems) é necessário para a funcionalidade de relatórios no formato PDF.
CSV	Exportação em valores separados por vírgulas, que pode ser usada para importação em muitos programas externos, como bancos de dados, planilhas e outros. Este relatório não permite selecionar o capítulo.
NBE export	Exportação delimitada por barras verticais, que pode ser usada para importação em muitos programas externos. Este relatório não permite selecionar o capítulo.

Depois de selecionar o formato, a caixa de diálogo “Save File” (Salvar arquivo) do navegador será exibida, permitindo que o usuário salve os resultados da varredura no local de sua escolha.

Para importar um relatório, clique no botão “**Upload**” (Fazer upload) na barra superior da tela “**Results**” (Resultados):



Com o botão “**Browse...**” (Procurar), selecione o arquivo de varredura **.nessus** que deseja importar e clique em “**Submit**” (Enviar). O Nessus analisará as informações e as disponibilizará na interface “**Results**” (Resultados).

Formato de arquivo **.nessus**

O Nessus usa um formato de arquivo específico (**.nessus**) para importar e exportar varreduras. Este formato tem as seguintes vantagens:

- É um arquivo do tipo XML compatível com versões anteriores e futuras e facilita a implementação.
- Autossuficiente: um único arquivo **.nessus** contém a lista de alvos e as políticas definidas pelo usuário, além dos próprios resultados da varredura.
- Seguro: as senhas não são salvas no arquivo. Em vez disso, usa-se uma referência a uma senha armazenada em um local seguro no host local.

O processo de criação de um arquivo **.nessus** que contém os alvos, as políticas e os resultados das varreduras é, primeiramente, gerar a política e salvá-la. Em seguida, gerar a lista de endereços de destino e, por último, executar uma varredura. Quando a varredura for concluída, todas as informações podem ser salvas em um arquivo **.nessus** com a opção “**Download**” da guia “**Reports**”. Consulte o documento “Formato de Arquivo Nessus v2” para obter mais detalhes sobre os arquivos **.nessus**.

Delete (Excluir)

Quando os resultados da varredura forem concluídos, selecione uma varredura na lista “**Results**” (Resultados), clique em “**Options**” (Opções) e clique no botão “**Delete Results**” (Excluir resultados). Isto excluirá a varredura da interface do

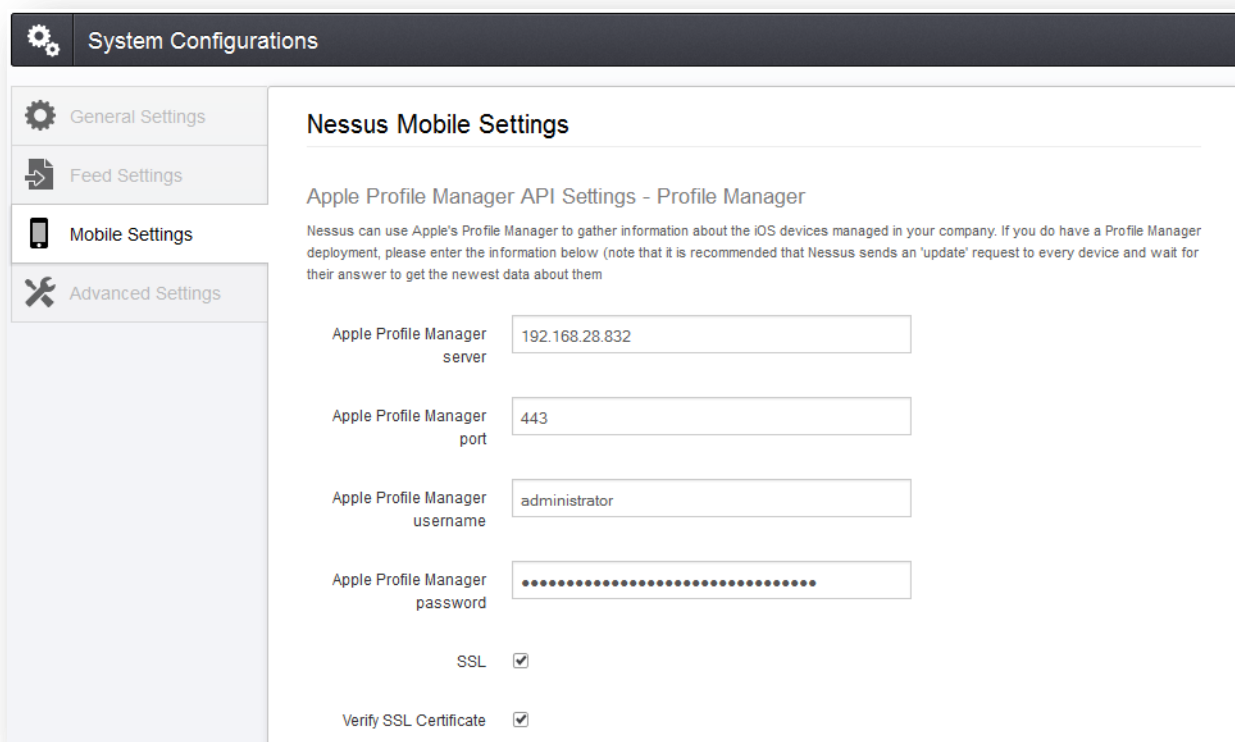
usuário. **Essa ação não pode ser desfeita.** Use o recurso “Download” para exportar os resultados de varredura antes da exclusão.

Móvel

O Nessus 5 tem capacidade para examinar [Active Directory Service Interfaces](#) e [Apple Profile Manager](#), permitindo o exame de inventário e vulnerabilidades de dispositivos baseados em Apple iOS e Android. O Nessus pode ser configurado para autenticar nesses servidores, consultar informações de dispositivos móveis e reportar questões.

Para procurar dispositivos móveis, o Nessus deve ser configurado com informações de autenticação para o(s) servidor(es) de gerenciamento.

O recurso de exame Mobile (Móvel) está especificado no menu “**Configuration**” (Configuração). A guia “Mobile Settings” (Configurações móveis) oferece um lugar único para configurar as informações de Apple Profile Manager e ADSI. Como o Nessus autentica diretamente nos servidores de gerenciamento, uma política para varreduras móveis será criada automaticamente com a família de plugins Mobile habilitada e uma varredura móvel será criada em “**Templates**” (Modelos). Usando a varredura modelo, os dispositivos móveis podem ser examinados com a frequência necessária.



The screenshot shows the 'System Configurations' window in Nessus. On the left is a sidebar with four settings categories: 'General Settings', 'Feed Settings', 'Mobile Settings' (which is selected and highlighted), and 'Advanced Settings'. The main content area is titled 'Nessus Mobile Settings'. Under the sub-header 'Apple Profile Manager API Settings - Profile Manager', there is a descriptive paragraph: 'Nessus can use Apple's Profile Manager to gather information about the iOS devices managed in your company. If you do have a Profile Manager deployment, please enter the information below (note that it is recommended that Nessus sends an 'update' request to every device and wait for their answer to get the newest data about them)'. Below this are four input fields: 'Apple Profile Manager server' with the value '192.168.28.832', 'Apple Profile Manager port' with '443', 'Apple Profile Manager username' with 'administrator', and 'Apple Profile Manager password' which is masked with dots. At the bottom, there are two checkboxes: 'SSL' and 'Verify SSL Certificate', both of which are checked.

SecurityCenter

Configuração do SecurityCenter 4.0-4.2 para funcionar com o Nessus

O “Nessus Server” pode ser adicionado por meio da interface de administração do SecurityCenter. Usando essa interface, o SecurityCenter pode ser configurado para acessar e controlar praticamente qualquer scanner Nessus. Clique na guia “Resources” (Recursos) e, em seguida, clique em “**Nessus Scanners**”. Clique em “**Add**” (Adicionar) para abrir a caixa de diálogo “Add Scanner” (Adicionar Scanner). O endereço IP do scanner Nessus, a porta do Nessus (padrão: 1241), o ID de login administrativo, o tipo de autenticação e a senha (criada durante a configuração do Nessus) são obrigatórios. Os campos de senha não estarão disponíveis se a autenticação “SSL Certificate” (Certificado SSL) for selecionada. Além disso, as zonas às quais o scanner Nessus será atribuído podem ser selecionadas.

Um exemplo de imagem da página “Add Scanner” do SecurityCenter é mostrado abaixo:

Nessus Scanners Home Resources Repositories Organizations Support Users Status Plugins

+ Add Scanner

Name: Local Scanner

Description: Local SecurityCenter Scanner

IP Address: 127.0.0.1

Port: 1241

Username: paul

Authentication Type: Password Based

Password: *****

Zones: 4Zone, 5Zone, .4and.5, .12Net, a

Cancel Submit

Depois de adicionar com êxito o scanner, a seguinte página é exibida após a seleção do scanner:

SecurityCenter ✓ Nessus Scanner "Local Scanner" was successfully added. Close Admin User System About Help Log out

Nessus Scanners Home Resources Repositories Organizations Support Users Status Plugins

+ Add **Edit** **Details** **Delete**

Name	IP	# of Zones	Status	Last Modified
Local Scanner	127.0.0.1	0	Working	Less than a minute ago

Consulte mais informações no “Guia de Administração do SecurityCenter”.

Configuração do SecurityCenter 4.4 para funcionar com o Nessus

A interface de administração do SecurityCenter é usada para configurar o acesso e controlar qualquer scanner Nessus, ou seja, versão 4.2.x ou superior. Clique na guia “**Resources**” (Recursos) e, em seguida, clique em “**Nessus Scanners**”. Clique em “**Add**” (Adicionar) para abrir a caixa de diálogo “**Add Scanner**” (Adicionar Scanner). O endereço IP ou nome do host do scanner Nessus, a porta do Nessus (padrão: 8834), as informações sobre o tipo de autenticação (criado durante a configuração do Nessus), a ID de login administrativo e a senha são obrigatórios. Os campos de senha não estarão disponíveis se a autenticação “SSL Certificate” (Certificado SSL) for selecionada. A capacidade de verificar o nome do host é fornecida para verificação do CommonName (CN) do certificado SSL apresentado pelo servidor Nessus. O estado do scanner Nessus pode ser definido como ativado ou desativado, conforme necessário (ativado é o padrão). As áreas do scanner Nessus podem ser atribuídas para seleção.

Um exemplo de imagem da página “Add Scanner” do SecurityCenter 4.4 é mostrado abaixo:

Nessus Scanners Home Resources Repositories Organizations Support Users Status Plugins

+ Add Scanner

Name:

Description:

Host:

Port:

Authentication Type:

Username:

Password:

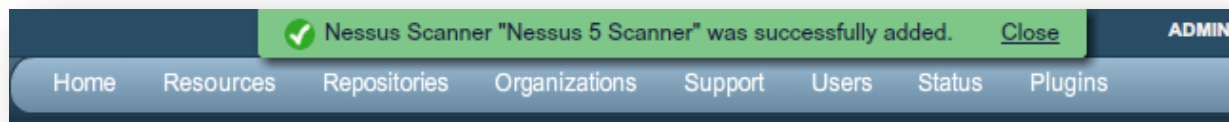
Verify Hostname: ☐

State: ☒ Enabled ☐ Disabled

Zones:

[Cancel](#) [Submit](#)

Depois de adicionar o scanner com êxito, o banner a seguir é exibido:



Para obter mais informações sobre como integrar o Nessus ao SecurityCenter, consulte o “Guia de Administração do SecurityCenter”.

Firewalls instalados no host

Se o servidor Nessus estiver configurado com um firewall local como ZoneAlarm, Sygate, BlackICE, firewall do Windows XP ou qualquer outro software de firewall, será necessário que as conexões sejam permitidas a partir do endereço IP do SecurityCenter.

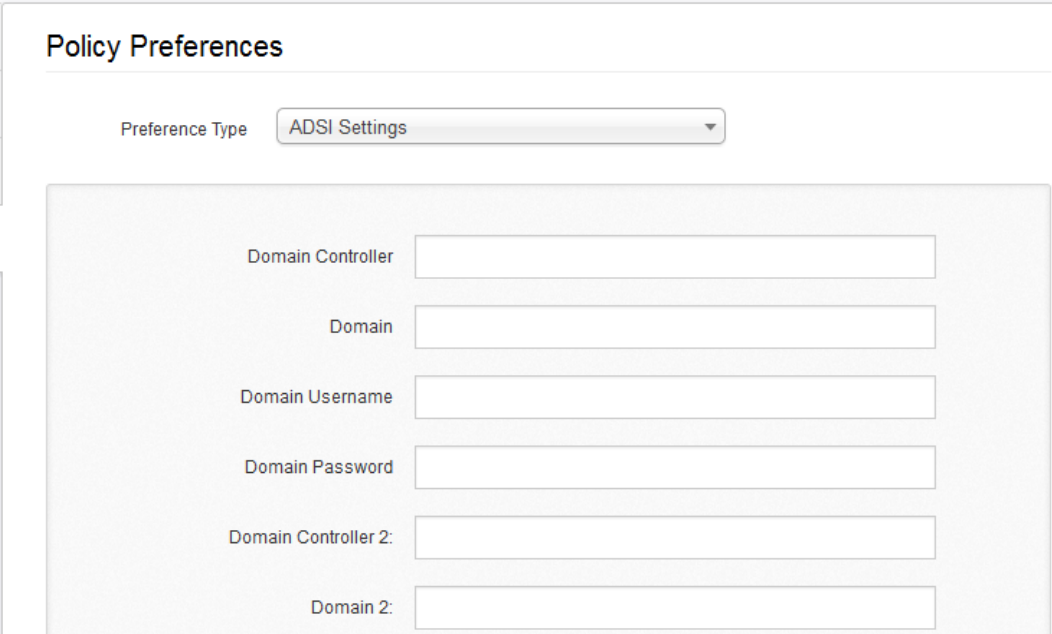
Normalmente, a porta 8834 é usada. Nos sistemas Microsoft XP Service Pack 2 e posteriores, clique em “**Security Center**” (Central de Segurança) no “**Control Panel**” (Painel de Controle) para gerenciar as configurações da opção “Firewall do Windows”. Para abrir a porta 8834, selecione a guia “**Exceptions**” (Exceções) e adicione a porta “8834” à lista.



Se o SecurityCenter usar o protocolo NTP obsoleto por meio da porta 1241, os comandos acima usariam 1241 em vez de 8834.

Verificação de preferências detalhadas

A guia “**Preferences**” (Preferências) em “**Policies**” (Políticas) contém 40 menus suspensos individualizados para configuração detalhada de varreduras. Recomenda-se reservar algum tempo para explorar e configurar cada menu para obter mais flexibilidade e resultados de verificação mais precisos com relação à política padrão. A seção a seguir oferece mais detalhes sobre cada opção “**Preferences**” (Preferências). Observe que esta é uma lista dinâmica de opções de configuração e depende do feed de plugins, das políticas de auditoria e de outras funções às quais o scanner Nessus conectado tem acesso. Um scanner com ProfessionalFeed pode ter opções de configuração mais avançadas do que um scanner configurado com o HomeFeed. Esta lista também pode mudar à medida que os plugins são adicionados ou modificados.



The screenshot shows the "Policy Preferences" window. At the top, there is a "Preference Type" dropdown menu set to "ADSI Settings". Below this, there are six input fields for domain-related settings:

- Domain Controller
- Domain
- Domain Username
- Domain Password
- Domain Controller 2:
- Domain 2:

“**ADSI Settings**” (Configurações ADSI) permite que o Nessus consulte um servidor ActiveSync para determinar se algum dispositivo Android ou iOS está conectado. Usando as credenciais e as informações de servidor, o Nessus autentica no controlador de domínio (e não no servidor Exchange) para consultá-lo diretamente sobre informações de dispositivos. Esse recurso não exige que quaisquer portas sejam especificadas na política de varredura. Essas configurações são obrigatórias para varreduras de dispositivos móveis.

Nota: Para “**ADSI Settings**” (Configurações ADSI) e “**Apple Profile Manager API Settings**” (Configurações da API do Apple Profile Manager), os dispositivos host não precisam ser examinados diretamente para obtenção de informações. O scanner Nessus deve ser capaz de alcançar o servidor MDM para consultá-lo quanto a informações. Quando uma dessas opções está configurada, a política para varreduras não exige um host de destino; você pode apontar para “localhost” e a política ainda conectará com o servidor MDM para obter informações.

Policy Preferences

Preference Type Apple Profile Manager API Settings ▾

Apple Profile Manager server

Apple Profile Manager port

Apple Profile Manager username

Apple Profile Manager password

SSL ☒

Verify SSL Certificate ☐

Force Device Updates ☒

Device Update Timeout (Minutes)

“Apple Profile Manager API Settings” (Configurações da API do Apple Profile Manager) permite que o Nessus consulte um servidor Apple Profile Manager para enumerar dispositivos baseados em Apple iOS (por exemplo, iPhone, iPad) na rede. Usando as credenciais e as informações de servidor, o Nessus autentica no Profile Manager para consultá-lo diretamente sobre informações de dispositivos. Ou então, é possível especificar comunicações por SSL, assim como direcionar o servidor para forçar uma atualização de informações de dispositivos (ou seja, cada dispositivo atualizará suas informações no servidor do Profile Manager).

Esse recurso não exige que quaisquer portas sejam especificadas na política de varredura. Essas configurações são obrigatórias para varreduras de dispositivos móveis.

Policy Preferences

Preference Type Apple Profile Manager API Settings ▼

Apple Profile Manager server

Apple Profile Manager port

Apple Profile Manager username

Apple Profile Manager password

SSL ☒

Verify SSL Certificate ☐

Force Device Updates ☒

Device Update Timeout (Minutes)

“Cisco IOS Compliance Checks” permite que os clientes do ProfessionalFeed enviem arquivos de políticas, que serão usados para determinar se um dispositivo Cisco IOS verificado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo. As políticas podem ser aplicadas com base nas configurações Salvo (**show config**), Em Execução (**show running**) ou Inicialização (**show startup**).

Policy Preferences

Preference Type Cisco IOS Compliance Checks

IOS Config File To Audit Saved/(show config)

Policy file #1 Browse...

Policy file #2 Browse...

Policy file #3 Browse...

Policy file #4 Browse...

Policy file #5 Browse...

“Database Compliance Checks” permite que os clientes do ProfessionalFeed enviem arquivos de políticas, que serão usados para determinar se um banco de dados testado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo.

Policy Preferences

Preference Type Database Compliance Checks

Policy file #1 Browse...

Policy file #2 Browse...

Policy file #3 Browse...

Policy file #4 Browse...

Policy file #5 Browse...

As opções “**Database settings**” (Configurações de banco de dados) são usadas para especificar o tipo de banco de dados a ser verificado e as configurações e credenciais correspondentes:

Opção	Descrição
Login	Nome de usuário do banco de dados.
Password	A senha para o nome de usuário fornecido.
DB Type	Oracle, SQL Server, MySQL, DB2, Informix/DRDA e PostgreSQL são permitidos.
Database SID	ID do banco de dados para auditoria.
Database port to use	Porta de escuta do banco de dados.
Oracle auth type	NORMAL, SYSOPER e SYSDBA são permitidos.
SQL Server auth type	Windows ou SQL são permitidos.

Policy Preferences

Preference Type
Database settings

Login

Password

DB Type

Oracle

Database SID

Database port to use

Oracle auth type:

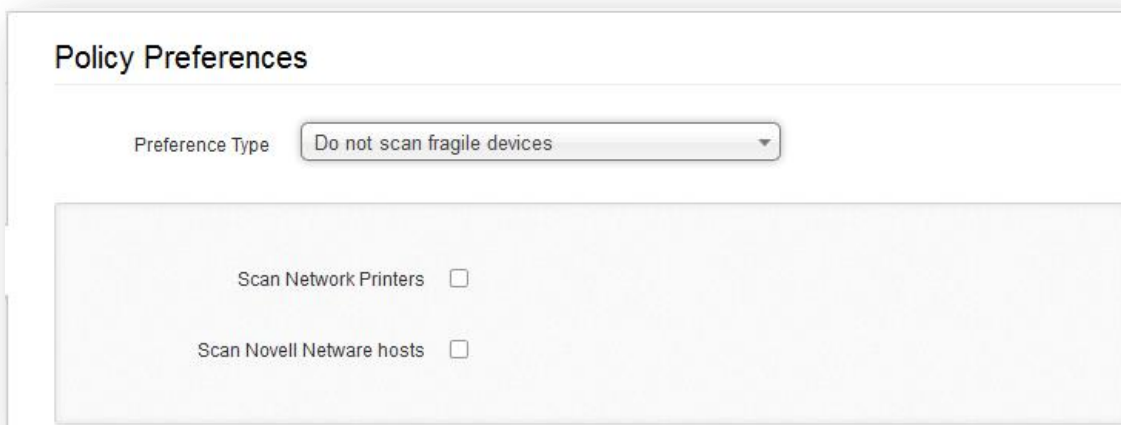
NORMAL

SQL Server auth type:

Windows

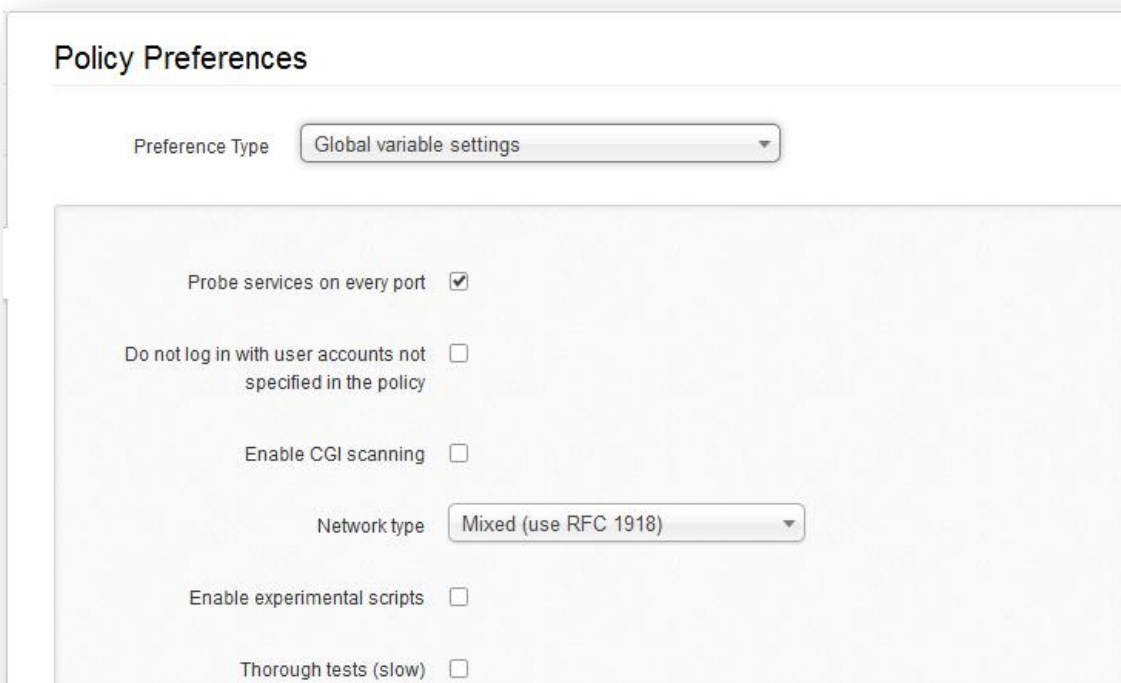
“**Do not scan fragile devices**” oferece duas opções, que instruem o scanner Nessus a não verificar um histórico de “fragilidade” ou propensão a falhas ao receber uma entrada inesperada. Os usuários podem selecionar “Scan Network

Printers” (Verificar impressoras em rede) ou “Scan Novell Netware hosts” (Verificar hosts Novell Netware) para instruir o Nessus a verificar esses dispositivos específicos. O Nessus só irá verificar as opções se estiverem marcadas. Recomenda-se que a verificação desses dispositivos seja realizada de maneira que permita às equipes de TI monitorar problemas nos sistemas.



The screenshot shows the 'Policy Preferences' window. At the top, the title 'Policy Preferences' is displayed. Below it, the 'Preference Type' dropdown menu is set to 'Do not scan fragile devices'. The main content area contains two options, both with unchecked checkboxes: 'Scan Network Printers' and 'Scan Novell Netware hosts'.

“Global variable settings” (Configurações de variáveis globais) contém uma grande variedade de opções de configuração para o servidor Nessus.



The screenshot shows the 'Policy Preferences' window with 'Global variable settings' selected in the 'Preference Type' dropdown. The main content area lists several configuration options: 'Probe services on every port' (checked), 'Do not log in with user accounts not specified in the policy' (unchecked), 'Enable CGI scanning' (unchecked), 'Network type' (dropdown menu set to 'Mixed (use RFC 1918)'), 'Enable experimental scripts' (unchecked), and 'Thorough tests (slow)' (unchecked).

A tabela a seguir fornece informações detalhadas sobre cada opção disponível:

Opção	Descrição
Probe services on every port	Relaciona cada porta aberta ao serviço que está sendo executado na porta. Observe que, em alguns casos raros, isto pode prejudicar alguns serviços e causar efeitos colaterais inesperados.
Do not log in with user accounts not specified in the policy	Usado para evitar o bloqueio de contas se a política de senhas estiver definida para bloquear as contas depois de algumas tentativas inválidas.
Enable CGI scanning	Ativa a varredura de CGI. Desative esta opção para acelerar a auditoria de uma rede local.
Network type	Permite especificar se os IPs públicos roteáveis, IPs roteáveis privados não pertencentes à Internet ou uma combinação de ambos estão em uso. Selecione "Mixed" (Combinado) se os endereços RFC 1918 forem usados com diversos roteadores de rede.
Enable experimental scripts	Faz com que os plugins "em teste" sejam usados na varredura. Não ative esta opção durante a varredura de uma rede de produção.
Thorough tests (slow)	Permite que os plugins realizem testes "completos". Por exemplo, ao examinar compartilhamentos de arquivos SMB, um plugin pode analisar com 3 níveis de profundidade em vez de 1. Isto pode aumentar o tráfego da rede e as análises, em alguns casos. Observe que, por ser mais completa, a varredura deve ser mais invasiva e é mais provável que afete a rede, mas os resultados de auditoria podem ser melhores.
Report verbosity	Um valor mais alto irá gerar mais ou menos informações sobre a atividade do plugin no relatório.
Report paranoia	Em alguns casos, o Nessus não pode determinar remotamente se uma falha está presente ou não. Se Report paranoia (Sensibilidade do relatório) for definido como "Paranoid" (Sensível), uma falha sempre será relatada, mesmo se houver dúvidas sobre o host remoto afetado. Por outro lado, a configuração de sensibilidade "Avoid false alarm" (Evitar alarmes falsos) fará com que o Nessus não comunique nenhuma falha sempre que houver uma sombra de incerteza sobre o host remoto. A opção ("Normal") é a configuração padrão entre as configurações acima.
HTTP User-Agent	Especifica o tipo de navegador que o Nessus representará durante a varredura.
SSL certificate to use	Permite que o Nessus use certificado SSL no lado cliente para se comunicar com um host remoto.
SSL CA to trust	Especifica a Autoridade Certificadora (CA) para confiabilidade do Nessus.
SSL key to use	Especifica uma chave SSL local que será usada para se comunicar com o host remoto.
SSL password for SSL key	A senha usada para gerenciar a chave SSL especificada.

Para facilitar os testes de aplicativos da Web, o Nessus pode importar cookies HTTP de um outro software (por exemplo, navegador, proxy de Web etc.) com as configurações "HTTP cookies import" (Importação de cookies HTTP). Um arquivo de cookie pode ser enviado para que o Nessus utilize cookies para acessar um aplicativo da Web. O arquivo do cookie deve estar no formato Netscape.

Policy Preferences

Preference Type: HTTP cookies import

Cookies file: Browse...

As configurações “**HTTP login page**” (Página de login de HTTP) permitem controlar o local em que os testes autenticados de um aplicativo de Web personalizado têm início.

Opção	Descrição
Login page	O URL básico para a página de login do aplicativo.
Login form	O parâmetro “action” do método do formulário. Por exemplo, o formulário de login de <code><form method="POST" name="auth_form" action="/login.php"></code> deve ser <code>"/login.php"</code> .
Login form fields	Especifica os parâmetros de autenticação (por exemplo, <code>login=%USER%&password=%PASS%</code>). Se as palavras-chaves <code>%USER%</code> e <code>%PASS%</code> forem usadas, serão substituídas por valores fornecidos no menu suspenso “Login configurations” (Configurações de login). Este campo pode ser usado para fornecer mais de dois parâmetros, se necessário (por exemplo, um nome de “grupo” ou alguma outra informação é necessária para o processo de autenticação).
Login form method	Especifica se a ação de login é realizada por meio de uma solicitação GET ou POST.
Automated login page search	Instrui o Nessus a pesquisar uma página de login.
Re-authenticate delay (seconds)	O intervalo entre as tentativas de autenticação. Previne o acionamento de mecanismos de bloqueio por força bruta.
Check authentication on page	O URL de uma página da Web protegida que requer autenticação para ajudar o Nessus a definir o status de autenticação.
Follow 30x redirections (# of levels)	Se um código de redirecionamento 30x for recebido de um servidor da Web, isso instruirá o Nessus a seguir o link fornecido ou não.
Authenticated regex	Um padrão regex para pesquisa na página de login. O recebimento de um código de resposta 200 nem sempre é suficiente para determinar o estado da sessão. O Nessus pode tentar localizar um determinado string, como “Authentication successful!” (Autenticação concluída).
Invert test (disconnected if regex matches)	Um padrão regex para pesquisa na página de login. Se for encontrado, indica ao Nessus que a autenticação não foi concluída (por exemplo, “Authentication failed!”).

Match regex on HTTP headers	O Nessus pode pesquisar um determinado padrão regex nos cabeçalhos de resposta HTTP para definir melhor o estado de autenticação, ao invés de pesquisar no corpo de uma resposta.
Case insensitive regex	Normalmente, as pesquisas por regex diferenciam maiúsculas de minúsculas. O comando instrui o Nessus a ignorar a diferenciação entre maiúsculas e minúsculas.
Abort web application tests if login fails	Se as credenciais fornecidas não funcionarem, o Nessus interromperá os testes personalizados de aplicativos da Web, mas não as famílias de plugins de CGI.

Policy Preferences

Preference Type
HTTP login page

Login page

/

Login form

Login form fields

user=%USER%&pass=%PASS%

Login form method

POST

Automated login page search

☐

Re-authenticate delay (seconds)

“**IBM iSeries Compliance Checks**” permite que os clientes do ProfessionalFeed enviem arquivos de políticas, que serão usados para determinar se um sistema IBM iSeries testado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo.

The screenshot shows a web interface titled "Policy Preferences". Below the title is a dropdown menu labeled "Preference Type" with the selected option "IBM iSeries Compliance Checks". The main content area contains five rows, each labeled "Policy file #1" through "Policy file #5". Each row has a text input field followed by a "Browse..." button.

As preferências de “**IBM iSeries Credentials**” proporcionam um local para que o Nessus forneça credenciais para autenticação do sistema IBM iSeries. Isto é necessário para auditorias de conformidade, por exemplo.

The screenshot shows a web interface titled "Policy Preferences". Below the title is a dropdown menu labeled "Preference Type" with the selected option "IBM iSeries Credentials". The main content area contains two rows: "Login" and "Password", each with a corresponding text input field.

O menu “**ICCP/COTP TSAP Addressing**” (Endereçamento ICCP/COTP TSAP) está relacionado especificamente às verificações Scada. O menu determina um valor de Pontos de Acesso de Serviço de Transporte (TSAP) do protocolo de Transporte Orientado a Conexões (COTP) em um servidor ICCP. Os valores de início e parada são definidos inicialmente como “8”.

The screenshot shows a web interface titled "Policy Preferences". Below the title is a dropdown menu labeled "Preference Type" with the selected option "ICCP/COTP TSAP Addressing Weakness". Below this, there are two input fields: "Start COTP TSAP" and "Stop COTP TSAP", both containing the value "8".

O menu “LDAP ‘Domain Admins’ Group Membership Enumeration” permite inserir um conjunto de credenciais LDAP, que podem ser usadas para enumerar uma lista de membros do grupo “Domain Admins” no diretório LDAP remoto.

The screenshot shows a web interface titled "Policy Preferences". Below the title is a dropdown menu labeled "Preference Type" with the selected option "LDAP 'Domain Admins' Group Membership E...". Below this, there are three input fields: "LDAP user", "LDAP password", and "Max results". The "Max results" field contains the value "1000". At the bottom of the form, there are two buttons: "Update" (in blue) and "Cancel" (in grey).

“**Login configurations**” (Configurações de Login) permite que o scanner Nessus use credenciais ao verificar HTTP, NNTP, FTP, POP2, POP3 ou IMAP. Ao fornecer credenciais, o Nessus pode realizar verificações mais abrangentes para determinar as vulnerabilidades. As credenciais de HTTP fornecidas aqui serão usadas apenas para autenticação básica e resumida. Para configurar as credenciais de um aplicativo da Web personalizado, use o menu suspenso “HTTP login page” (Página de login HTTP).

The screenshot shows a web interface titled "Policy Preferences". Below the title is a dropdown menu labeled "Preference Type" with "Login configurations" selected. The main content area contains six input fields arranged in two columns. The left column labels are "HTTP account", "HTTP password (sent in clear)", "NNTP account", "NNTP password (sent in clear)", "FTP account", and "FTP password (sent in clear)". The right column shows the values: an empty field for HTTP account, an empty field for HTTP password, an empty field for NNTP account, an empty field for NNTP password, the text "anonymous" for FTP account, and a field filled with dots for FTP password.

Field Label	Value
HTTP account	
HTTP password (sent in clear)	
NNTP account	
NNTP password (sent in clear)	
FTP account	anonymous
FTP password (sent in clear)	

As opções “**Modbus/TCP Coil Access**” estão disponíveis para os usuários do ProfessionalFeed. Este item de menu é gerado dinamicamente pelos plugins SCADA disponíveis com o ProfessionalFeed. O Modbus usa o código de função 1 para ler “bobinas” em um escravo Modbus. As bobinas representam configurações de saída binárias e normalmente são correlacionadas com atuadores. A capacidade de ler bobinas pode permitir a um atacante criar um perfil do sistema, identificar intervalos de registros e alterá-los por meio de uma mensagem “write coil” (gravar bobina). Os valores padrão são “0” para o reg Start e “16” para o reg End.

The screenshot shows the same "Policy Preferences" window, but the "Preference Type" dropdown is now set to "Modbus/TCP Coil Access". The main content area contains two input fields. The first is labeled "Start reg" and has the value "0". The second is labeled "End reg" and has the value "16".

Field Label	Value
Start reg	0
End reg	16

As opções “**Nessus SYN scanner**” e “**Nessus TCP scanner**” permitem configurar os scanners SYN e TCP originais para detectar a presença de um firewall.

Valor	Descrição
Automatic (normal)	Esta opção pode ajudar a identificar se um firewall está localizado entre o scanner e o destino (padrão).
Disabled (softer)	Desativa o recurso Firewall detection (Detecção de firewall).
Do not detect RST rate limitation (soft)	Desativa a funcionalidade de monitoramento do número de reinícios definidos e determina se há uma limitação configurada por um dispositivo de rede local.
Ignore closed ports (aggressive)	Tenta executar os plugins mesmo que a porta esteja fechada. Recomenda-se que esta opção não seja usada em uma rede de produção.

Preference Type

Firewall detection

Preference Type

Firewall detection

A opção “**News Server (NNTP) Information Disclosure**” (Divulgação de Informações do Servidor de Notícias (NNTP)) pode ser usada para determinar a existência de servidores de notícias capazes de distribuir spam. O Nessus tentará publicar uma mensagem ao(s) servidor(es) de notícias NNTP (Protocolo de Transporte de Notícias em Rede) para verificar se é possível enviar uma mensagem a servidores de notícias em um ponto da rede remota.

Opção	Descrição
From address	O endereço que o Nessus usará ao tentar enviar uma mensagem ao(s) servidor(es) de notícias. Essa mensagem será excluída automaticamente após um breve intervalo de tempo.
Test group name regex	Nome do grupo de notícias que receberá uma mensagem de teste do endereço especificado. O nome pode ser especificado como uma expressão regular (regex), para que a mensagem possa ser enviada simultaneamente a vários grupos de notícias. Por exemplo, o valor padrão “ f[a-z].tests? ” transmitirá uma mensagem de e-mail a todos os grupos de notícias com nomes que começam com qualquer letra (de “a” a “z”) e terminam com “.tests” (ou alguma variação que corresponda ao string). O ponto de interrogação age como um caractere curinga opcional.
Max crosspost	O número máximo de servidores de notícias que receberão a publicação de teste, independentemente do número de correspondências de nomes. Por exemplo, se o crosspost Max for “ 7 ”, a mensagem de teste será enviada apenas a sete servidores de notícias, mesmo que haja 2.000 servidores de notícias correspondentes ao regex neste campo.
Local distribution	Se esta opção for selecionada, o Nessus tentará enviar apenas uma mensagem ao(s) servidor(es) de notícias local(is). Caso contrário, tentará encaminhar a mensagem a um ponto remoto.

No archive

Se esta opção for selecionada, o Nessus solicitará para não arquivar a mensagem de teste enviada ao(s) servidor(es) de notícias. Caso contrário, a mensagem será arquivada como qualquer outra publicação.

Policy Preferences

Preference Type: News Server (NNTP) Information Disclosure

From address: Nobody <nobody@example.com>

Test group name regex: f[a-z]\.tests?

Max crosspost: 7

Local distribution: ☒

No archive: ☐

“Oracle Settings” (Configurações do Oracle) configura o Nessus com o Oracle Database SID e inclui uma opção para testar contas padrão conhecidas no software da Oracle.

Policy Preferences

Preference Type: Oracle Settings

Oracle SID:

Test default accounts (slow): ☐

“PCI DSS Compliance” fará com que o Nessus compare os resultados das varreduras com as normas de conformidade PCI DSS vigentes. Este recurso está disponível apenas para os clientes do ProfessionalFeed.

Policy Preferences

Preference Type: PCI DSS compliance

Check for PCI-DSS compliance ☐

O Nessus pode explorar credenciais para o servidor Red Hat Satellite, WSUS, SCCM e sistemas de gerenciamento de patches VMware Go (anteriormente Shavlik) para realizar a auditoria de patches nos sistemas nos quais as credenciais não estão disponíveis para o scanner Nessus. As opções dos sistemas de gerenciamento de patches “Preferences” podem ser encontradas em seus respectivos menus suspensos: **Patch Management: Red Hat Satellite Server Settings**, **“Patch Management: SCCM Server Settings”**, **“Patch Management: VMware Go Server Settings”** e **“Patch Management: WSUS Server Settings”**. Para obter mais informações sobre como utilizar o Nessus para verificar os hosts por meio desses sistemas de gerenciamento de patch, consulte o documento [“Patch Management Integration”](#).

As opções **“Ping the remote host”** (Teste de ping para o host remoto) permitem um controle individualizado sobre a capacidade do Nessus de enviar testes de conexão a hosts durante a varredura de descoberta. Isto pode ser feito com ping ARP, ping TCP, ping ICMP ou ping UDP de aplicativo.

Opção	Descrição
TCP ping destination port(s)	Especifica a lista de portas a serem verificadas por meio do teste de ping TCP. Se tiver dúvidas com relação às portas, deixe esta configuração com o valor padrão “interno”.
Number of Retries (ICMP)	Permite especificar o número de tentativas de ping ao host remoto. O valor padrão é 6.
Do an applicative UDP ping (DNS, RPC...)	Executa um teste de ping UDP em aplicativos específicos que usam UDP, incluindo DNS (porta 53), RPC (porta 111), NTP (porta 123) e RIP (porta 520).
Make the dead hosts appear in the report	Se esta opção for selecionada, os hosts que não responderam à solicitação de ping serão incluídos no relatório de segurança como hosts “inativos”.
Log live hosts in the report	Selecione esta opção para comunicar especificamente a capacidade de enviar um ping a um host remoto.
Test the local Nessus host	Esta opção permite que o usuário inclua ou exclua o host do Nessus local da varredura. Esta opção é usada quando o host Nessus estiver dentro do intervalo de rede de destino da varredura.
Fast network discovery	Normalmente, ao enviar um “ping” a um IP remoto com uma resposta, o Nessus realiza varreduras adicionais para verificar se não se trata de um proxy transparente ou um balanceador de carga gerando ruído, mas sem resultado (alguns dispositivos respondem a todas as portas de 1 a 65.535, mas não há nenhum serviço em segundo plano). As verificações podem demorar um pouco, especialmente se o host remoto estiver protegido por um firewall. Se a “descoberta rápida de rede” estiver ativada, o Nessus não realizará as varreduras.



Para examinar os sistemas VMware convidados, o “ping” deve ser desativado. Na política de varredura em “Advanced” (Avançado) -> “Ping the remote host” (Ping para o host remoto), desmarque o ping de TCP, ICMP e ARP.

Policy Preferences

Preference Type: Ping the remote host

TCP ping destination port(s): built-in

Do an ARP ping: ☒

Do a TCP ping: ☒

Do an ICMP ping: ☒

Number of retries (ICMP): 2

Do an applicative UDP ping (DNS,RPC...): ☐

“**Patch Management**” (Gerenciamento de patches) fornece diversas opções para usar servidores de gerenciamento de patches de terceiros para consultar hosts quanto a informações de vulnerabilidade. Mais informações sobre essas opções de configuração estão disponíveis no documento “[Patch Management Integration](#)” (Integração de gerenciamento de patches).

“**Port scanner settings**” (Configurações do scanner de portas) oferece duas opções adicionais para controlar a atividade de varredura de portas:

Opção	Descrição
Check open TCP ports found by local port enumerators	Se um enumerador de portas locais (por exemplo, WMI ou netstat) encontrar uma porta, o Nessus também verificará se está aberta remotamente. Isto ajuda a determinar se alguma forma de controle de acesso está em uso (por exemplo, TCP wrappers, firewall).
Only run network port scanners if local port enumeration failed	Nesse caso, use primeiro a enumeração de portas locais.

Policy Preferences

Preference Type Port scanners settings

Check open TCP ports found by local port enumerators ☐

Only run network port scanners if local port enumeration failed ☒

“**SMB Registry: Start the Registry Service during the scan**” (Registro de SMB: Iniciar o Serviço de Registro durante a varredura) permite que o serviço intermedeie algumas das exigências de varredura para computadores em que o registro SMB não funcione todo o tempo.

No menu “**SMB Scope**” (Escopo de SMB), se a opção “**Request information about the domain**” (Solicitar informações sobre o domínio) estiver selecionada, os usuários do domínio, não os usuários locais, serão consultados.

Preference Type SMB Registry : Start the Registry Service dur...

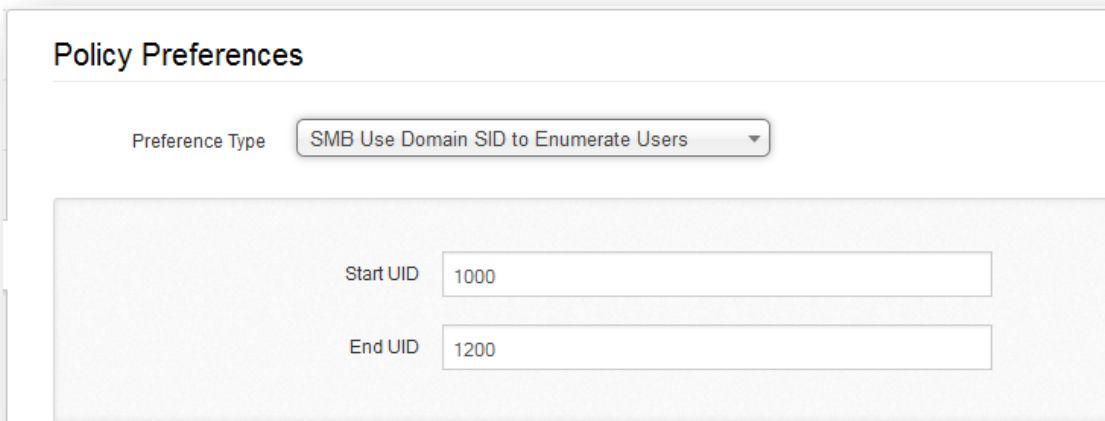
Start the registry service during the scan ☐

Enable administrative shares during the scan ☐

Preference Type SMB Scope

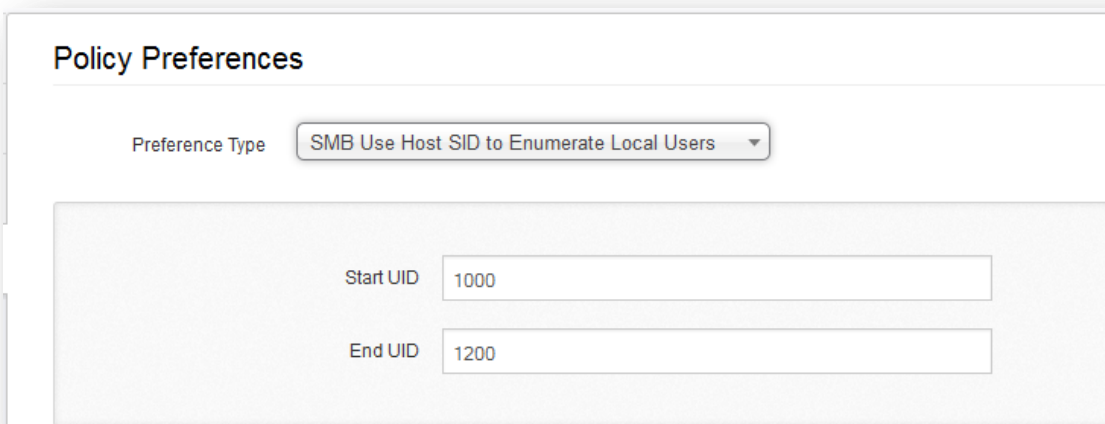
Request information about the domain ☒

“**SMB Use Domain SID to Enumerate Users**” (SMB usa o SID de Domínio para Enumerar Usuários) especifica o intervalo de SID a ser usado para realizar uma consulta inversa de nomes de usuários no domínio. A configuração padrão é recomendada para a maioria das varreduras.



The screenshot shows a window titled "Policy Preferences". Inside, there is a section labeled "Preference Type" with a dropdown menu set to "SMB Use Domain SID to Enumerate Users". Below this, there are two input fields: "Start UID" with the value "1000" and "End UID" with the value "1200".

“**SMB Use Host SID to Enumerate Local Users**” (SMB usa o SID de Host para Enumerar Usuários) especifica o intervalo de SID a ser usado para executar uma consulta inversa de nomes de usuários locais. A configuração padrão é recomendada.



The screenshot shows a window titled "Policy Preferences". Inside, there is a section labeled "Preference Type" with a dropdown menu set to "SMB Use Host SID to Enumerate Local Users". Below this, there are two input fields: "Start UID" with the value "1000" and "End UID" with the value "1200".

“**SMTP settings**” (Configurações de SMTP) especifica as opções para os testes de SMTP (Protocolo Simples de Transporte de Correio) executados em todos os dispositivos dentro do domínio verificado que estão executando serviços SMTP. O Nessus tentará retransmitir mensagens por meio do dispositivo ao domínio de terceiros especificado (“**Third party domain**”). Se a mensagem enviada a “**Third party domain**” for recusada pelo endereço especificado no campo “To address” (Endereço de destino), ocorrerá falha na tentativa de spam. Se a mensagem for aceita, o servidor de SMTP foi usado com sucesso para retransmitir o spam.

Opção	Descrição
Third party domain	O Nessus tentará enviar spam por meio de cada dispositivo de SMTP para o endereço listado neste campo. O endereço de domínio de terceiros deve estar fora do intervalo do site que está sendo examinado ou do site que está realizando a varredura. Caso contrário, o teste pode ser interrompido pelo servidor SMTP.
From address	As mensagens de teste enviadas ao(s) servidor(es) SMTP aparecerão como se fossem originadas do endereço especificado neste campo.
To address	O Nessus tentará enviar mensagens endereçadas ao destinatário da mensagem indicado neste campo. O endereço postmaster é o valor padrão, pois é um endereço válido na maioria dos servidores de correio.

Policy Preferences

Preference Type SMTP settings

Third party domain

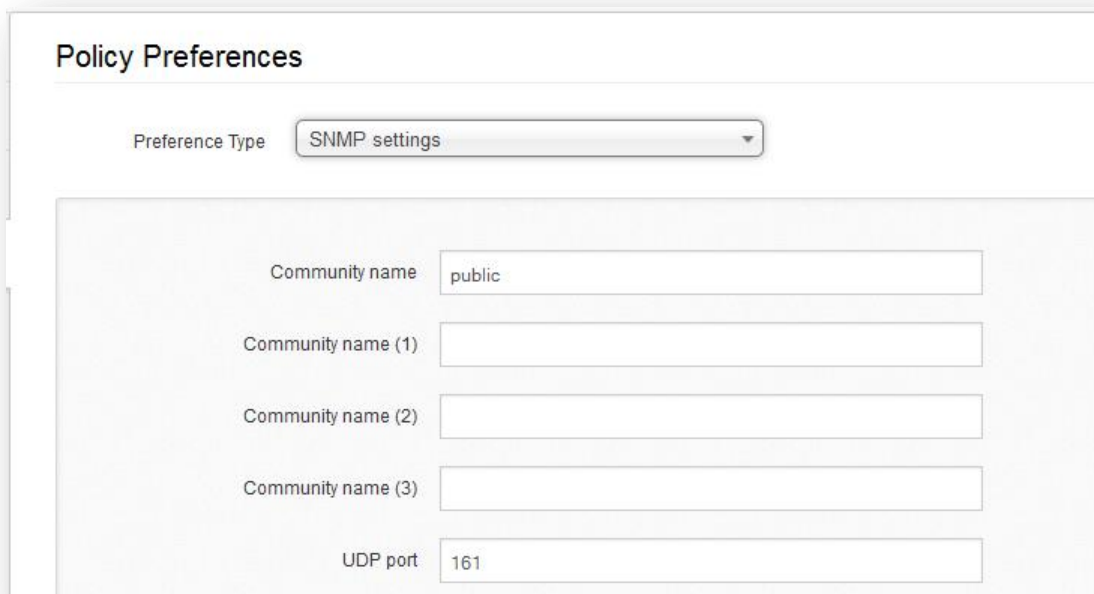
From address

To address

“**SNMP settings**” (Configurações de SNMP) permite configurar o Nessus para se conectar e autenticar no serviço SNMP do destino. Durante a varredura, o Nessus fará algumas tentativas de descobrir o string da comunidade e usá-la em testes subsequentes. Até quatro strings de nomes de comunidades separadas podem ser usados por política de varredura. Se o Nessus não localizar o string e/ou a senha da comunidade, não poderá realizar uma auditoria completa do serviço.

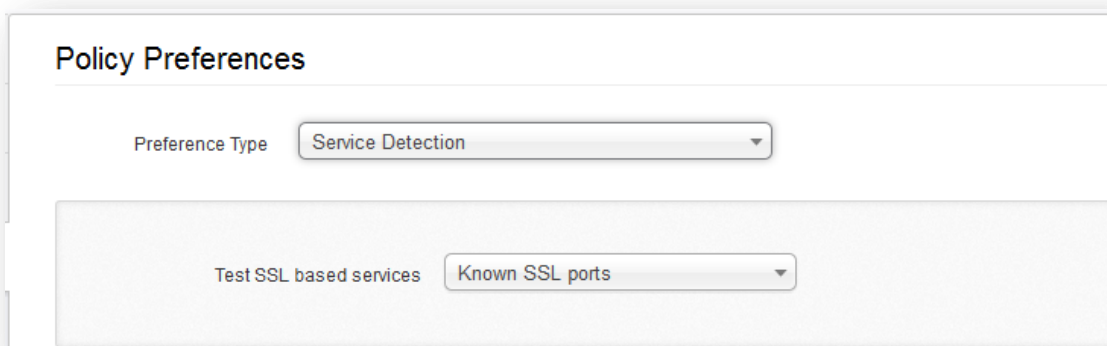
Opção	Descrição
Community name (0-3)	O nome da comunidade SNMP.
UDP port	Instrui o Nessus a verificar uma porta diferente caso o SNMP esteja sendo executado em uma porta que não seja a porta 161.
SNMPv3 user name	O nome de usuário de uma conta que usa SNMPv3.
SNMPv3 authentication password	A senha do nome de usuário especificado.
SNMPv3 authentication algorithm	Selecione MD5 ou SHA1, dependendo do algoritmo reconhecido pelo serviço remoto.

SNMPv3 privacy password	A senha usada para proteger a comunicação SNMP criptografada.
SNMPv3 privacy algorithm	O algoritmo de criptografia a ser usado para o tráfego SNMP.



The screenshot shows the 'Policy Preferences' window. At the top, the title 'Policy Preferences' is displayed. Below it, there is a 'Preference Type' dropdown menu set to 'SNMP settings'. The main area contains several input fields: 'Community name' with the value 'public', 'Community name (1)', 'Community name (2)', 'Community name (3)', and 'UDP port' with the value '161'.

“**Service Detection**” (Detecção de Serviços) controla o modo como o Nessus testará serviços SSL: portas SSL conhecidas (por exemplo, 443), todas as portas ou nenhuma. O teste de funcionalidade SSL em todas as portas pode afetar o host verificado.



The screenshot shows the 'Policy Preferences' window. At the top, the title 'Policy Preferences' is displayed. Below it, there is a 'Preference Type' dropdown menu set to 'Service Detection'. The main area contains a 'Test SSL based services' dropdown menu set to 'Known SSL ports'.

“**Unix Compliance Checks**” permite que os clientes do ProfessionalFeed enviem arquivos de auditoria do Unix, que serão usados para determinar se um sistema testado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo.

The screenshot shows a 'Policy Preferences' window. At the top, there is a 'Preference Type' dropdown menu set to 'Unix Compliance Checks'. Below this, there are five rows, each labeled 'Policy file #1' through 'Policy file #5'. Each row consists of a text input field followed by a 'Browse...' button.

“**VMware SOAP API Settings**” fornece as credenciais necessárias ao Nessus para autenticação dos sistemas de gerenciamento VMware ESX, ESXi e vSphere Hypervisor por meio do seu próprio API SOAP, uma vez que o acesso SSH tenha sido descontinuado. O API foi projetado para auditoria de hosts do vSphere 4.x / 5.x, ESXi e ESX, mas *não* das máquinas virtuais em funcionamento nos hosts. Este método de autenticação pode ser usado para realizar varredura com credenciais ou auditorias de conformidade.

The screenshot shows a 'Policy Preferences' window. At the top, there is a 'Preference Type' dropdown menu set to 'VMware SOAP API Settings'. Below this, there are three fields: 'VMware user name' with a text input field, 'VMware password (unsafe!)' with a text input field, and 'Ignore SSL Certificate' with an unchecked checkbox.

Opção	Descrição
VMware user name	Nome do usuário para autenticação. As credenciais podem ser contas do Active Directory (AD) para hosts integrados ou contas locais e a conta deve estar no grupo root local. As credenciais de domínio são user@domain e as contas locais são usuário e senha.

VMware password (unsafe!)	Esta senha é enviada de forma insegura e pode ser interceptada por meio de "sniffing" da rede.
Ignore SSL Certificate	Se um certificado SSL estiver presente no servidor, ignore-o.

“Wake-on-LAN” (WOL) controla os hosts que receberão pacotes "mágicos" WOL antes de realizar uma varredura, além do tempo de espera (em minutos) para a inicialização dos sistemas. A lista de endereços MAC do WOL é inserida por meio de um arquivo de texto enviado com um endereço MAC de host por linha. Por exemplo,

```
00:11:22:33:44:55
aa:bb:cc:dd:ee:ff
[...]
```

Policy Preferences

Preference Type: Wake-on-LAN

List of MAC addresses for Wake-on-LAN: Browse...

Time to wait (in minutes) for the systems to boot: 5

“Web Application Tests Settings” (Configurações dos Testes de Aplicativos da Web) verifica os argumentos das CGIs (Common Gateway Interfaces) remotas descobertas no processo de espelhamento de Web ao tentar enviar erros comuns de programação de CGI, como cross-site scripting, inclusão remota de arquivos, execução de comandos, ataques transversais ou injeção de SQL. Ative esta opção marcando a caixa de seleção “Enable web applications tests” (Ativar testes de aplicativos da Web). Os testes dependem dos seguintes plugins NASL:

- [11139](#), [42424](#), [42479](#), [42426](#), [42427](#), [43160](#) – Injeção de SQL (abuso de CGI)
- [39465](#), [44967](#) – Execução de comandos (abuso de CGI)
- [39466](#), [47831](#), [42425](#), [46193](#), [49067](#) – Cross-Site Scripting (abuso de CGI: XSS)
- [39467](#), [46195](#), [46194](#) – Directory Traversal (abuso de CGI)
- [39468](#) – HTTP Header Injection (abuso de CGI: XSS)
- [39469](#), [42056](#), [42872](#) – Inclusão de arquivo (abuso de CGI)
- [42055](#) – String de formato (abuso de CGI)
- [42423](#), [42054](#) – Server Side Includes (abuso de CGI)
- [44136](#) – Cookie Manipulation (abuso de CGI)

- [46196](#) – XML Injection (abuso de CGI)
- [40406](#), [48926](#), [48927](#) – Mensagens de erro
- [47830](#), [47832](#), [47834](#), [44134](#) – Ataques adicionais (abuso de CGI)

Nota: Esta lista de plugins relacionados a aplicativos da Web é atualizada com frequência e pode não ser completa. Os plugins adicionais podem depender das configurações desta opção de preferência.

Opção	Descrição
Maximum run time (min)	Esta opção gerencia o tempo (em minutos) usado na execução de testes de aplicativos da Web. O valor inicial desta opção é 60 minutos e se aplica a todas as portas e CGIs de um determinado website. A varredura de websites da rede local com aplicativos pequenos normalmente é realizada em menos de uma hora. No entanto, websites com aplicativos maiores podem exigir um valor maior.
Try all HTTP methods	Normalmente, o Nessus só irá realizar os testes com solicitações GET. Esta opção também instruirá o Nessus a usar “POST requests” para testes de formulários da Web aprimorados. Normalmente, os testes de aplicativos da Web usarão apenas solicitações GET, a menos que esta opção esteja ativada. Em geral, aplicativos mais complexos usam o método POST quando um usuário envia dados ao aplicativo. Esta configuração permite um teste mais completo, mas pode aumentar consideravelmente o tempo exigido. Se esta opção for selecionada, o Nessus testará cada script/variável com as solicitações GET e POST.
Combinations of arguments values	Esta opção gerencia a combinação de valores dos argumentos usados nas solicitações de HTTP. Este menu suspenso possui três opções: one value – Testa um parâmetro por vez com um string de ataque sem tentar variações de parâmetros adicionais “sem ataque”. Por exemplo, o Nessus tentaria aplicar “/test.php?arg1=XSS&b=1&c=1”, onde “b” e “c” permitem outros valores, sem testar cada combinação. Este é o método mais rápido de teste com o menor conjunto de resultados gerados. All pairs (slower but efficient) – Esta forma de teste é um pouco mais lenta, mas é mais eficaz que o teste “one value”. Ao verificar diversos parâmetros, verifica também o string de ataque, as variações de uma única variável e usa o primeiro valor com todas as outras variáveis. Por exemplo, o Nessus tenta aplicar “/test.php?a=XSS&b=1&c=1&d=1” e percorre as variáveis, de modo que uma receba o string de ataque e a outra redefina todos os valores possíveis (conforme descoberto durante o processo de espelhamento), e qualquer outra variável recebe o primeiro valor. Neste caso, o Nessus nunca testará “/test.php?a=XSS&b=3&c=3&d=3” quando o primeiro valor de cada variável for “1”. All combinations (extremely slow) – Este método de teste realiza um teste completo de todas as combinações possíveis de sequências de ataque com entrada válida nas variáveis. Enquanto o teste “All-pairs” (Todos os pares) cria um conjunto menor de dados para maior desempenho, esta opção é bastante lenta, pois usa um conjunto completo de dados de testes. Esse método de teste pode levar muito tempo para ser concluído.

HTTP Parameter Pollution	Ao realizar testes de aplicativos da Web, esta opção tenta contornar qualquer mecanismo de filtragem por meio da injeção de conteúdo em uma variável enquanto fornece a mesma variável com conteúdo válido. Por exemplo, um teste de injeção SQL normal pode ter o seguinte aspecto: <code>"/target.cgi?a='&b=2"</code> . Com a opção HTTP Parameter Pollution (HPP) ativada, a solicitação pode parecer a seguinte: <code>"/target.cgi?a='&a=1&b=2"</code> .
Stop at first flaw	Esta opção determina um ataque em uma nova falha. Isto é feito no nível do script. A detecção de uma falha de XSS não desativará as pesquisas de injeção de SQL ou injeção de cabeçalho, mas haverá, no máximo, um relatório para cada tipo em uma determinada porta, a menos que "thorough tests" (testes completos) esteja definido. Observe que várias falhas do mesmo tipo (por exemplo, XSS, SQLI etc.) podem ser relatadas às vezes, se forem detectadas pelo mesmo ataque. O menu suspenso possui quatro opções: per CGI – Assim que uma falha é encontrada em uma CGI por um script, o Nessus passa à CGI conhecida seguinte no mesmo servidor ou, se não houver outras CGIs, à porta/servidor seguinte. Esta é a opção padrão. per port (quicker) – Assim que uma falha é encontrada em um servidor Web por um script, o Nessus para e alterna para o outro servidor Web em uma porta diferente. per parameter (slow) – Quando um tipo de falha é encontrado em um parâmetro de uma CGI (por exemplo, XSS), o Nessus alterna para o parâmetro seguinte da mesma CGI ou da CGI conhecida ou para a porta/servidor seguinte. look for all flaws (slower) – Execute testes completos, independentemente das falhas encontradas. Esta opção pode gerar um relatório muito detalhado e, na maioria dos casos, não é recomendável.
Test Embedded web servers	Os servidores Web incorporados são, muitas vezes, estáticos e não contêm scripts de CGI personalizáveis. Além disso, os servidores da Web incorporados podem travar ou deixar de responder quando passam por uma varredura. A Tenable recomenda que os servidores Web incorporados sejam examinados separadamente de outros servidores Web com esta opção.
URL for Remote File Inclusion	Durante testes de inclusão remota de arquivos (RFI), esta opção especifica um arquivo em um host remoto para ser usado nos testes. Por padrão, o Nessus usará um arquivo seguro hospedado no servidor da Web da Tenable para os testes de RFI. Se o scanner não tiver acesso à Internet, recomenda-se usar um arquivo hospedado internamente para realizar testes mais precisos de RFI.

Policy Preferences

Preference Type Web Application Tests Settings

Enable web applications tests ☐

Maximum run time (min)

Try all HTTP methods ☐

Combinations of arguments values one value

HTTP Parameter Pollution ☐

Stop at first flaw per CGI

Test embedded web servers ☐

URL for Remote File Inclusion

“Web Mirroring” (Espelhamento de Web) define os parâmetros de configuração para o utilitário original de espelhamento de conteúdo do servidor Web do Nessus. O Nessus realiza o espelhamento do conteúdo da Web para aprimorar a análise de vulnerabilidades e ajudar a reduzir o impacto sobre o servidor.



Se os parâmetros de espelhamento da Web forem definidos de maneira a espelhar um site inteiro, o aumento significativo do tráfego poderá ocorrer durante a varredura. Por exemplo, se houver 1 gigabyte de material em um servidor Web e o Nessus estiver configurado para espelhar todo o conteúdo, a varredura irá gerar pelo menos 1 gigabyte de tráfego do servidor para o scanner Nessus.

Opção	Descrição
Number of pages to mirror	Número máximo de páginas a espelhar.
Maximum depth	Limita o número de links que o Nessus seguirá em cada página inicial.
Start page	O URL da primeira página a ser verificada. Se forem necessárias várias páginas, use dois pontos para separá-las (por exemplo, “/:/php4:/base”).
Excluded items regex	Permite que partes do website não estejam sujeitas ao rastreamento. Por exemplo, para excluir o diretório “/manual” e todas as CGIs Perl, defina esse campo como: <code>(^/manual) (\.pl (\?.*) ?\$) .</code>
Follow dynamic pages	Se esta opção for selecionada, o Nessus seguirá os links dinâmicos e poderá exceder os parâmetros definidos acima.

Policy Preferences

Preference Type Web mirroring

Number of pages to mirror

Maximum depth

Start page

Excluded items regex

Follow dynamic pages ☐

“**Windows Compliance Checks**” permite que os clientes do ProfessionalFeed enviem arquivos de auditoria do Microsoft Windows, que serão usados para determinar se um sistema testado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo.

Policy Preferences

Preference Type Windows Compliance Checks

Policy file #1 Browse...

Policy file #2 Browse...

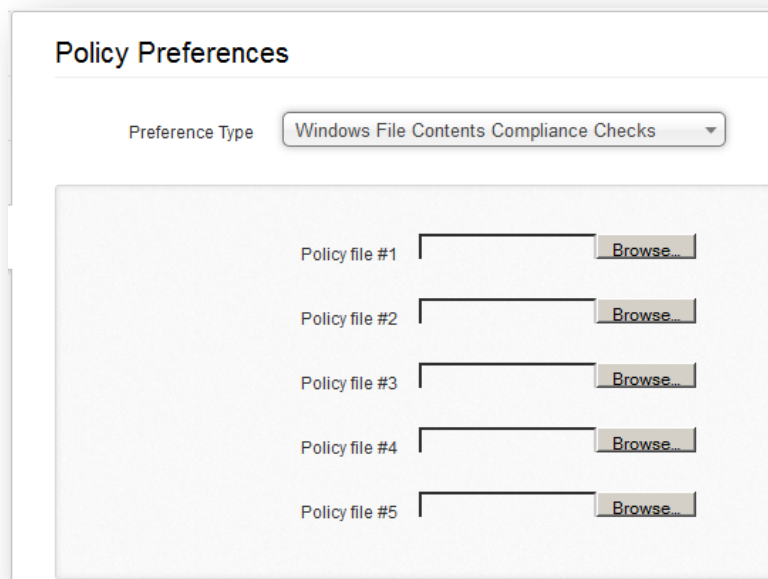
Policy file #3 Browse...

Policy file #4 Browse...

Policy file #5 Browse...

“**Windows File Contents Compliance Checks**” (Verificações de Conformidade do Conteúdo de Arquivos do Windows) permite que os clientes do ProfessionalFeed enviem arquivos de auditoria do Windows, que pesquisam tipos específicos de conteúdos no sistema (por exemplo, cartões de crédito, números de documentos de identidade) para ajudar a determinar o cumprimento de normas internas da empresa ou normas externas.

Quando todas as opções forem configuradas da maneira desejada, clique em “**Submit**” (Enviar) para salvar a política e voltar à guia Policies (Políticas). A qualquer momento, clique em “**Edit**” (Editar) para fazer alterações em uma política criada ou clique em “**Delete**” (Excluir) para excluir completamente uma política.



Policy Preferences

Preference Type: Windows File Contents Compliance Checks

Policy file #1 Browse...

Policy file #2 Browse...

Policy file #3 Browse...

Policy file #4 Browse...

Policy file #5 Browse...

Para obter mais informações

A Tenable possui vários documentos que descrevem a instalação, implementação, configuração, operação do usuário e testes gerais do Nessus. O documentos estão listados a seguir:

- **Guia de Instalação do Nessus** – instruções passo a passo da instalação.
- **Verificações de Credenciais do Nessus para Unix e Windows** – informações sobre como realizar varreduras autenticadas de rede com o scanner de vulnerabilidades Nessus.
- **Verificações de Conformidade do Nessus** – guia geral para compreender e executar verificações de conformidade com o Nessus e o SecurityCenter.
- **Referência de Verificações de Conformidade do Nessus** – guia completo da sintaxe das verificações de conformidade do Nessus.
- **Formato de arquivo Nessus v2** – descreve a estrutura do formato de arquivo **.nessus**, que foi introduzido com o Nessus 3.2 e NessusClient 3.2.
- **Especificação do protocolo Nessus XML-RPC** – descreve o protocolo e a interface XML-RPC do Nessus.
- **Monitoramento de Conformidade em Tempo Real** – descreve como as soluções da Tenable podem ser usadas para ajudar a cumprir muitos tipos diferentes de normas do governo e do setor financeiro.
- **Guia de Administração do SecurityCenter**

Outros recursos on-line são listados a seguir:

- Fórum de discussão do Nessus: <https://discussions.nessus.org/>

- Blog da Tenable: <http://blog.tenable.com/>
- Podcast da Tenable: <http://blog.tenablesecurity.com/podcast/>
- Vídeo de exemplos de uso: <http://www.youtube.com/user/tenablesecurity>
- Feed do twitter da Tenable: <http://twitter.com/tenablesecurity>

Entre em contato conosco pelo e-mail support@tenable.com, sales@tenable.com ou visite nosso site no endereço <http://www.tenable.com/>.

Sobre a Tenable Network Security

Tenable Network Security, líder em monitoramento unificado de segurança, é a criadora do scanner de vulnerabilidades Nessus e de soluções de primeira classe sem agente para o monitoramento contínuo de vulnerabilidades, pontos fracos de configuração, vazamento de dados, gerenciamento de logs e detecção de comprometimentos para ajudar a garantir a segurança da rede e o cumprimento das leis e normas FDCC, FISMA, SANS CSIS e PCI. Os produtos premiados da Tenable são utilizados por muitas organizações da Global 2000 e por órgãos públicos para tomar a iniciativa de reduzir os riscos nas redes. Para mais informações, visite <http://www.tenable.com/>.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com

